ATLANTIS LAND
where solutions begin

WIRELESS ROUTER ADSL2+

A02-RA241-W54

MANUEL D'INSTALLATION

A02-RA241-W54_MF01

Copyright

Copyright. 2002 est la propriété de cette société. Tout droits réservés. Sont interdites, la reproduction, la transmission, la transcription, la mémorisation dans un système de sauvegarde où la traduction dans une autre langue ou en langage informatique quels qu'ils soient, de la présente publication, sous quelque forme que ce soit ou quelque en soit le moyen, électronique, mécanique, magnétique, optique, chimique, manuel ou de tout autre genre, sans avoir obtenu préalablement l'autorisation de notre entreprise.

Non-responsabilité

La présente entreprise n'admet ni requêtes ni de garantie, explicites ou implicites, au sujet du contenu et de manière spécifique exclue la possibilité de garantie, communicabilité ou adaptabilité pour des finalités particulières. Le logiciel décrit dans le présent manuel est vendu ou concédé en licence "tel quel". Si les programmes devaient présenter des problèmes après l'achat, l'acquéreur (et non pas la présente entreprise, son distributeur ou concessionnaire) est tenu de prendre en charge tous les coûts de manutention ainsi que les coûts dus à des dommages accidentels ou des conséquences dérivants d'un défaut du logiciel. La présente entreprise se réserve en outre le droit de revoir le contenu de cette publication et d'y apporter des modifications de temps en temps, sans obligation d'informer les utilisateurs de ces changements. Nous avons fait tout notre possible afin d'éviter la présence d'erreurs dans le texte, les images, les tableaux présents dans ce manuel et dans le Cd-Rom. Cependant, nous ne pouvons pas garantir l'absence totale d'erreurs et/ou d'omissions, nous vous remercions donc de nous les signaler et vous prions de nous en excuser. Enfin, nous ne pouvons être tenus pour responsables dans quelque perte que ce soit, dommage ou incompréhension à la suite directe ou indirecte de l'utilisation de notre manuel, le logiciel Cd-Rom et/ou disque dur.

Toutes les marques ou noms de produits mentionnés dans le présent manuel sont des marques commerciales et/ou brevetées par leurs propriétaires respectifs.

Marquage CE

Cet appareil, qui appartient à la Classe B peut causer des interférences radio, dans ce cas nous vous invitons à prendre les contre-mesures appropriées.

ATTENTION

Laisser au moins 30 cm de distance entre les antennes du dispositif et les utilisateurs.

FCC

Cet appareil est conforme à la quinzième partie des Règles de la FCC (Class B). Son fonctionnement est soumis à deux conditions :

- Il ne doit pas provoquer d'interférences gênantes.
- Il ne doit pas subir d'interférences, et notamment pas d'interférences susceptibles d'entraîner un fonctionnement anormal.

Ces limites sont étudiées de manière à assurer une protection correcte contre les interférences gênantes en zone résidentielle. Cet équipement produit, utilise et peut émettre de l'énergie en fréquences radio. S'il n'est pas installé et utilisé conformément aux instructions, il peut provoquer des perturbations des communications radio. L'absence de perturbations ne peut cependant pas être garantie pour une configuration donnée. Si l'appareil perturbe la réception de la radio ou de la télévision (ce qui peut être déterminé en l'éteignant puis en le remettant sous tension), l'utilisateur peut prendre les mesures suivantes pour corriger ces interférences :

- Réorienter ou déplacer l'antenne réceptrice.

• Augmenter la distance entre le récepteur et l'équipement.
• Brancher l'équipement dans une prise située sur un circuit différent de celui auquel le récepteur est connecté.
• Demander conseil au revendeur ou à un technicien radio-télévision expérimenté.

SOMMAIRE

CHAPITRE 1 1

1.1 CARACTERISTIQUES PRINCIPALES 1
1.2 DANS LA BOITE 2
1.3 PRINCIPALES CARACTERISTIQUES TECHNIQUES 2
1.4 CABLAGE 2

CHAPITRE 2 2

2.1 PRECAUTIONS GENERALES POUR L'USAGE DU ROUTEUR 2
2.2 FACE AVANT 2
2.3 FACE ARRIERE 3

CHAPITRE 3 4

3.1 AVANT DE COMMENCER 4
3.2 CONFIGURATION DU TCP/IP 4
Configuration sous Windows 95/98/ME 4
Configuration sous Windows NT4.0 6
Configuration sous Windows 2000 7
Configuration sous Windows XP 9
3.3 VERIFICATION 11
3.4 CONFIGURATION INITIALE 11
3.4.1 Mot de Passe et Login 11
3.4.2 Ports LAN et WAN 12
3.5 FAI 12
3.6 CONFIGURATION AVEC LE NAVIGATEUR 12
3.6.1 STATUT (STATUS) 13
3.6.1.1 Table ARP 13
3.6.1.2 Table de Routage 14
3.6.1.3 Table DHCP 15
3.6.1.4 Evénement Système 15
3.6.1.5 Evénements de Sécurité 15
3.6.2 Guide d'installation rapide 17
3.6.3 CONFIGURATION 19
3.6.3.1 LAN 19
3.6.3.1.1 Ethernet 19
3.6.3.1.2 Wireless 20
3.6.3.1.3 Wireless Security 21
3.6.3.1.4 Serveur DHCP 23
3.6.3.2 WAN 25
3.6.3.2.1 ISP 25
3.6.3.2.2 DNS 32
3.6.3.2.3 ADSL 32
3.6.3.3 SYSTEME (System) 33
3.6.3.3.1 Base de temps (Time Zone) 33

3.6.3.3.2 Remote Access 33
3.6.3.3.3 Mise à jour (Firmware Upgrade) 34
3.6.3.3.4 Backup / Restore 34
3.6.3.3.5 Redémarrage (Restart) 35
3.6.3.3.6 Mot de passe (User Management) 36
3.6.3.4 Pare Feu (Firewall) 37
3.6.3.4.1 Filtrage de paquets (Packet Filtering) 37
3.6.3.4.2 Filtrage par adresse Mac (Mac Filtering) 44
3.6.3.4.3 Detection d'Intrusion (Intrusion Detection) 46
3.6.3.4.4 Blocage d'adresse Wan (Block Wan Request) 46
3.6.3.4.5 Filtrage par Url (URL Filtering) 47
3.6.3.5 QoS 48
3.6.3.6 Serveur Virtuel 60
3.6.3.7 Fonctions avancées 62
3.6.3.7.1 Static Route 62
3.6. 3.7.2 Dynamic DNS 63
3.6.3.7.3 Contrôle VLAN 64
3.6.3.7.4 Device Management 64
3.6.3.7.5 IGMP 66
3.6.4 Sauvegarde en mémoire (Save Config to Flash) 67

CHAPITRE 4 68

PROBLEMES AU DEMARRAGE DU WIRELESS ADSL ROUTER 68
MOT DE PASSE? 68
IMPOSSIBLE D'ENTRER DANS LE ROUTER PAR LE WEB 69
PROBLEMES AVEC L'INTERFACE LAN 69
PROBLEMES AVEC L'INTERFACE WAN 69
PROBLEMES DE CONNEXION A UN NOEUD DISTANT OU A UN FAI 70
CONFLITS D'ADRESSES IP 70
LE ROUTER NE PEUT PAS SE POSITIONNER? 71
QU'EST CE QUE LE NAT? 71
PAQUETS IP 72
UNE APPLICATION INTERNET NE FONCTIONNE PAS CORRECTEMENT 72
POURQUOI MEME AVEC LE SERVEUR VIRTUEL DES APPLICATIONS NE MARCHENT PAS? 73
POURQUOI MEME AVEC LE DMZ DES APPLICATIONS NE MARCHENT PAS? 73
RFC 1483 BRIDGE AVEC MAC OS 9 73
RFC 1483 BRIDGE AVEC MAC OS X 74
RFC 1483 BRIDGE AVEC WINDOWS 95, 98, ME 74
RFC 1483 BRIDGE AVEC WINDOWS 2000 75
RFC 1483 BRIDGE AVEC LINUX 75
LES PERFORMANCES DU ROUTER NE SONT PAS BONNES 75
QU'EST CE QUE LE RELAIS DHCP ? 75
QU'EST CE QUE C'EST LE TEMPS DE MISE AU REPOS? 76
POURQUOI LE WIRELESS ROUTER ADSL2+ SE CONNECTE AUTOMATIQUEMENT A L'ISP? 76
QU'EST CE QU'UNE ATTAQUE DE DENI DE SERVICE? 77
QU'EST CE QU'UNE ATTAQUE DENIAL OF SERVICE? 77
COMMENT EMPECHER A UN GROUPE D'UTILISATEURS DE SURFER SUR INTERNET? 78
QU'EST CE QUE LE DDNS? 79
EST-CE QUE JE PEUX DEMARRER UNE APPLICATION D'UN ORDINATEUR SATELLITE PRESENT DANS LE RESEAU WIRELESS?? 80

EST –CE QUE JE PEUX JOUER EN RESEAU AVEC LES AUTRES ORDINATEURS PRESENTS DANS LE WLAN? 80
QU'EST-CE QUE C'EST LE SPREAD SPECTRUM? 80
QU'EST-CE QUE C'EST DSSS ET FHHS? 81
PEUVENT LES INFORMATIONS ENVOYEES PAR WIRELESS ETRE INTERCEPTEES? 81
QU'EST-CE QUE C'EST WEP? 81
QU'EST-CE QUE C'EST INFRASTRUCTURE MODE? 81
QU'EST-CE QUE C'EST ISM BAND? 82
QU'EST-CE QUE C'EST LE STANDARD IEEE 802.11G? 82

APPENDICE A 83

DYNAMIQUE DNS 83

APPENDICE B 85

FILTRAGE DE PAQUETS 85

APPENDICE C 88

CONSIDERATIONS SUR LES RESEAUX SANS FIL (WIRELESS) 88

APPENDICE D 90

UNIVERSEL PNP 90

APPENDICE E 92

CARACTERISTIQUES AVANÇEES 92

APPENDICE F 93

SUPPORT 93

Chapitre 1
Introduction

Ce manuel a été rédigé pour une utilisation avancée du Wireless Router ADSL2+, pour cette raison y sont abordés des sujets qui peuvent rebuter certains utilisateurs.
Pour une configuration rapide, il est conseillé d'utiliser le « Guide à l'Installation » présent sur le CDROM et sur support papier (installation et câblage, configuration du PC et de la connexion ADSL du Routeur) ainsi que la Video.

1.1 Caractéristiques Principales

Partager une Connexion Haut Debit
Le Compact Router ADSL2+ (grâce à son modem ADSL2+ intégré) permet jusqu'à 24 Mbps en flux descendant. Il dispose de 4 ports Fast Ethernet (avec auto-détection 10/100 Mbps) pour la connexion directe à 4 ordinateurs ou au réseau. Doté de la fonctionnalité NAT, il permet aux différents utilisateurs de partager simultanément la connexion ADSL en n'utilisant qu'un seul abonnement avec le fournisseur d'accès internet et qu'une seule adresse IP.

Mobilité / Wireless
Le Wireless Router ADSL est la solution complète et idéale, qui permet une navigation sans fil en utilisant une seule connexion ADSL, de partager les données et de se mouvoir en toute liberté.
Il est donc possible d'ajouter à votre réseau LAN actuel (sans préoccupation de câbles encombrants et chers) jusqu'à 253 utilisateurs en les connectant (sans fil) malgré des obstacles tels que murs et cloisons (l'algorithme de cryptage WPA assure une transmission sécurisée).

Pare-feu et VLAN
Il intègre un pare-feu sophistiqué avec les fonctionnalités avancées d'inspection de paquets et blocage d'URL. Il peut automatiquement reconnaître et bloquer les attaques de type Déni de Service (DoS) et il détermine si un paquet de données qui arrive peut être envoyé dans le Lan. Le VLAN permet de segmenter le trafic du réseau en améliorant sa gestion et surtout ses performances. De plus il augmente la sécurité globale du réseau LAN.

Qualité du Service et IP Throttling
Le Routeur a la capacité d'acheminer les informations issues des applications en fonction de leur priorité. Plusieurs Classes de Services sont proposées, et à chaque type vous pouvez affecter une priorité en fonction de vos exigences de qualité de service.
La vitesse de la navigation ne sera plus ralentie à cause des programmes P2P utilisés sur d'autres ordinateurs.

Gestion et Configuration facile
En utilisant le navigateur Web, vous pouvez configurer facilement le Compact Router ADSL2+, à partir de n'importe quelle station du réseau local ou via Internet, indépendamment du type d'abonnement ADSL grâce au client Dynamique DNS intégré.

1.2 Dans la boîte

Une fois ouverte, vous devriez trouver les éléments suivants:

- Wireless Routeur ADSL2+
- Câble réseau (CAT5)
- Câble RJ11
- Alimentation (12V, 1A)
- CD-Rom avec manuels et software
- Guide d'installation rapide
- Coupon de Garantie

Si vous constatez qu'un de ces composants manque, merci de vous adressez à votre revendeur.

1.3 Principales Caractéristiques Techniques

Interfaces Matérielles

- 4 ports LAN Fast Ethernet
- 1 port WAN RJ11 pour la connection ADSL/ADSL2/ADSL2+
- 9 LEDs pour diagnostic immédiat
- Interrupteur Marche/Arrêt et Bouton Reset

Interface Wireless

- Fréquence: plage 2.4GHz - 2.436GHz
- Conforme aux spécificités IEEE 802.11g et IEEE 802.11b
- Chipset: ImproComm™
- Vitesse de transmission: jusqu'à 54Mbps
- Cryptage WPA et WEP (64/128bit)
- Antenne externe orientable

Standard ADSL/ATM/PROTOCOLES

- ADSL Chipset TreandChip3162™ (Compatible avec les DSLAM les plus diffusés)
- Standards ADSL: ADSL Multi-Mode standard [ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2)]
- Standard ADSL2 : ITU G.992.3 (G.dmt.bis)
- Standard ADSL2+ : ITU G.992.5 (G.dmt.bisplus)
- Standards ATM: AAL5 and ATM service class:UBR, CBR, VBR-rt, VBR et OAM F4/F5 loopback
- Supports: VC-based et LLC-based multiplexing
- ATM/ADSL Protocoles: Bridge & Routed Ethernet over ATM (RFC 2684, 1483), PPPoE (RFC2516),
- PPPoA (RFC2364), RFC1577

Pare feu / Firewall
- Filtrage par Paquet, Adresse Mac et URL
- Prévention du Deni de service, Inspection des paquets (SPI) et Détection d'intrusion

VPN
- IPSec et PPTP pass-through

Gestion
- Guide rapide d'installation
- Interface par naviguateur WEB et Console pour gestion locale, Telnet pour locale et à distance
- FTP & TFTP pour mise à jour du firmware

Protocole Réseau
- Nat, RIP1/2 & routage statique
- Serveur Virtuel, Universel Plug&Play (UPnP) & DMZ
- Serveur, Client & Relais DHCP / Relais DNS

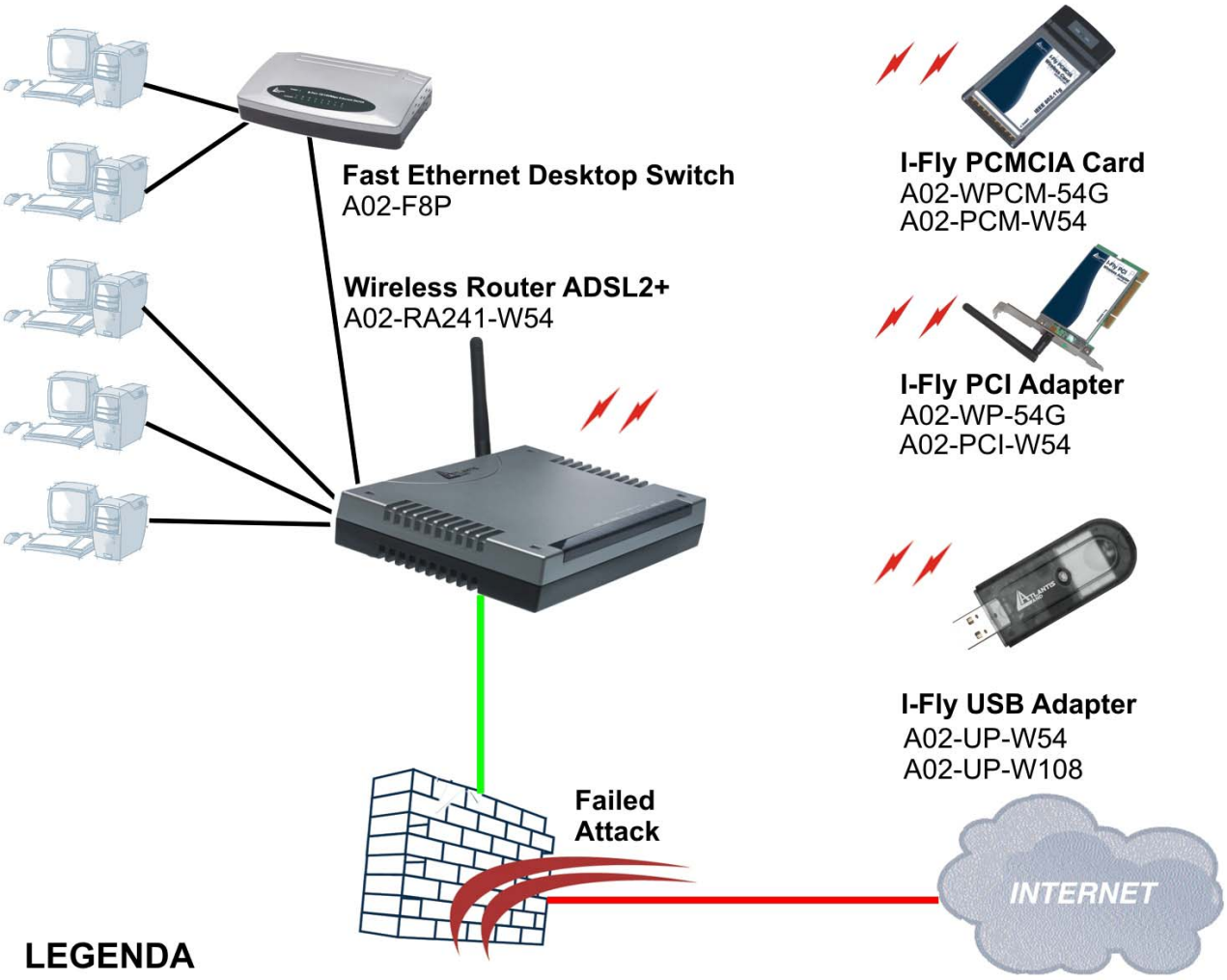
Caractéristiques Avançées
- Dynamique DNS
- VLAN
- QoS

Dimensions et environnement
- Alimentation: Externe 12VDC/1A
- Dimensions: 180x120x32 mm
- Temperature de Fonctionnement: 0 ~ 40 C / Humidité 10-95% (sans condensation)

Contenu de la boîte:
- Router-Modem-Access point Wireless Lan 802.11g
- CD-Rom vec le manuel (Français, Italien et Anglais)
- Guide d'installation rapide (Français, Italien et Anglais)
- Câble RJ11, Câble réseau (CAT5) et Adaptateur secteur (12V,1A)

1.4 Câblage

Après avoir terminé le câblage, raccordez l'alimentation pour mettre le Wireless Routeur ADSL2+ sous tension. Assurez-vous que les LEDs sont correctement allumées. Connectez un câble réseau (standard ou croisé) pour relier le Routeur à un Hub/Switch ou à un PC. Une fois toutes les liaisons effectuées et le Wireless Routeur ADSL2+ allumé, le produit effectuera un diagnostic (d'une soixantaine de secondes). Quand cette étape sera terminée, les Leds PWR, SYS seront allumées, ce qui signifie que le produit fonctionne correctement. Enfin, la Led ADSL clignotera en vert pour indiquer la phase d'alignement puis se stabilera (condition indispensable pour naviguer sur internet). Vous devez installer un filtre à toutes les prises téléphoniques utilisées par un téléphone/fax.

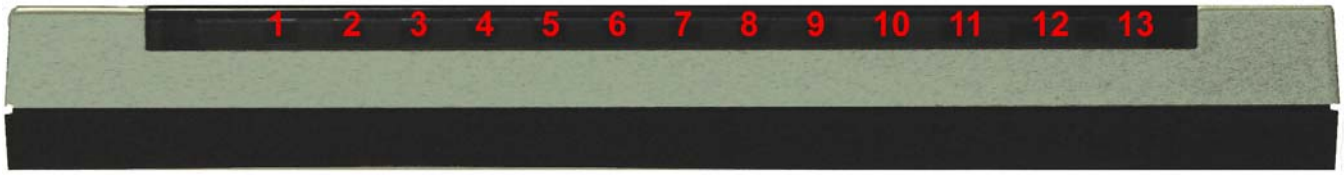

Fast Ethernet Desktop Switch
A02-F8P
Wireless Router ADSL2+
A02-RA241-W54
I-Fly PCMCIA Card
A02-WPCM-54G
A02-PCM-W54
I-Fly PCI Adapter
A02-WP-54G
A02-PCI-W54
I-Fly USB Adapter
A02-UP-W54
A02-UP-W108
Failed
Attack
INTERNET
LEGENDA
INTERNET
10/100Mbps
WIRELESS
54Mbps

Chapitre 2
Usage du Routeur Wireless ADSL

2.1 Précautions générales pour l'usage du Routeur

Ne pas utiliser le Wireless Routeur ADSL2+ dans un endroit exposé à des conditions de température et d'hygrométrie élevées, le Wireless Routeur ADSL2+ pourrait fonctionner de manière incorrecte et/ou subir des dommages.
Ne pas utiliser la même prise électrique pour alimenter d'autres appareils.
Ne pas ouvrir le boitier du Wireless Routeur ADSL2+ r, ni tenter de le réparer seul.
Si le Wireless Routeur ADSL2+ est trop chaud, vous devez l'éteindre immédiatement et vous adresser à du personnel qualifié.
Mettre le Wireless Routeur ADSL2+ sur une surface plate et stable.
Utiliser exclusivement l'alimentation fournie dans l'emballage.
Pour effectuez la mise à jour du firmware, vous devez utiliser une connexion filaire.

2.2 Face avant



LED	Signification
POWER (5)	Allumée quand le Routeur est sous tension.
SYS (6)	Clitognante pour indiquer que le système est actif.
WLAN (7)	Clignotante pour indiquer la transmission de données ou le fonctionnement correct du module wireless.
LAN (8-11)	Allumée quand le LAN (réseau) est connecté Verte = connexion à 100Mbps Orange = connexion à 10Mbps Clignote lors des transferts de données.
ADSL (12)	Fixe, elle indique une connexion correcte. Clignotante, en cours de connection.
PPP (13)	Fixe, elle indique une connexion PPP active.

2.3 Face arrière

PORT	USAGE
LINE (RJ-11)	Connectez le câble (fourni) RJ11 au filtre ADSL (optionnel) et enfin à la prise téléphonique
LAN (4*RJ-45)*	Reliez directement avec un câble Ethernet (standard ou croisé) aux PC ou à un Hub/Switch.
RESET	Lorsque le routeur est allumé, pressez cette touche pendant environ 10 secondes pour effectuer le reset puis redemarrer le routeur par la touche Power On/Off.
POWER (Jack)	Connectez l'alimentation fournie
POWER Switch	Pressez pour allumer / éteindre le Routeur

Chapitre 3
Configuration

En utilisant le navigateur Web, vous pouvez configurer facilement le Wireless Routeur ADSL2+. De plus, vous pouvez le gérer à partir de n'importe quelle station du réseau local ou via Internet.

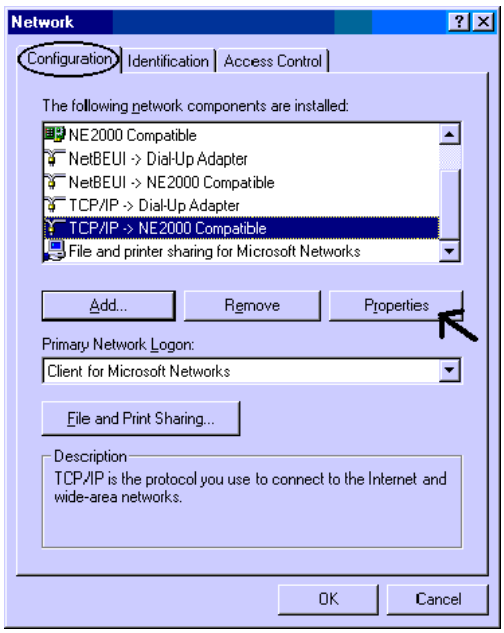
3.1 Avant de Commencer

Tous les PC doivent avoir une carte réseau (Fast Ethernet ou Wireless) correctement installée, au moins l'un d'entre eux doit être joint au Wireless Routeur ADSL2+ directement ou par un Hub/Switch et avoir le protocole TCP/IP installé.

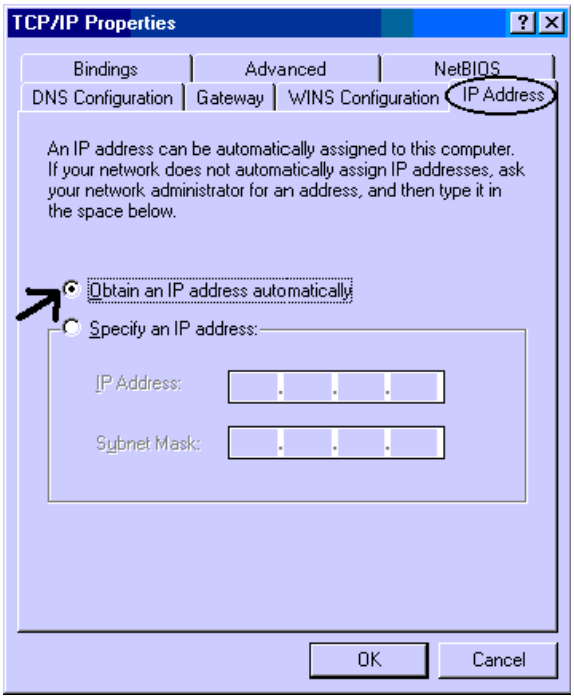
3.2 Configuration du TCP/IP

Configuration sous Windows 95/98/ME

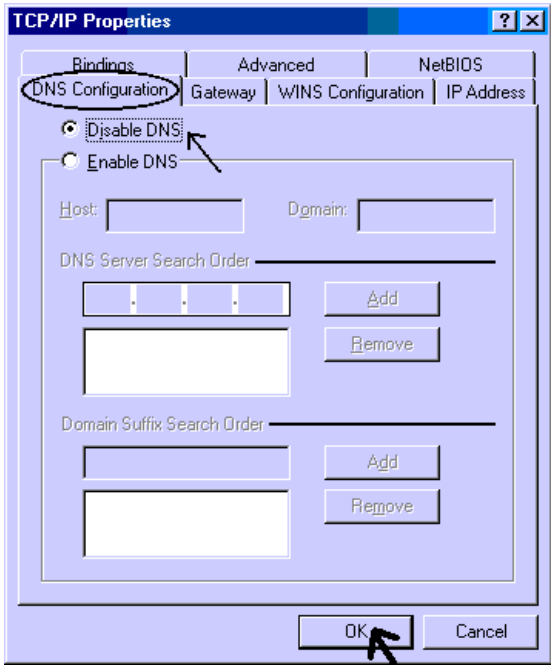
1. Allez dans **Panneau de Configuration**. Double-cliquez sur **Réseau**.et afficher l'onglet **Configuration**.
2. Sélectionnez le protocole **TCP/IP -> NIC carte**, ou une carte réseau Ethernet du PC.
3. Cliquez sur **Propriétés**



4. Dans l'onglet **Adresse IP** Sélectionnez l'option **Obtenir automatiquement une adresse IP** .


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

5. Sélectionnez l'onglet **DNS**.
6. Sélectionnez l'option **Désactiver DNS** puis cliquez sur **OK** pour terminer la configuration. Vous devez redémarrer l'ordinateur pour que les changements prennent effet.

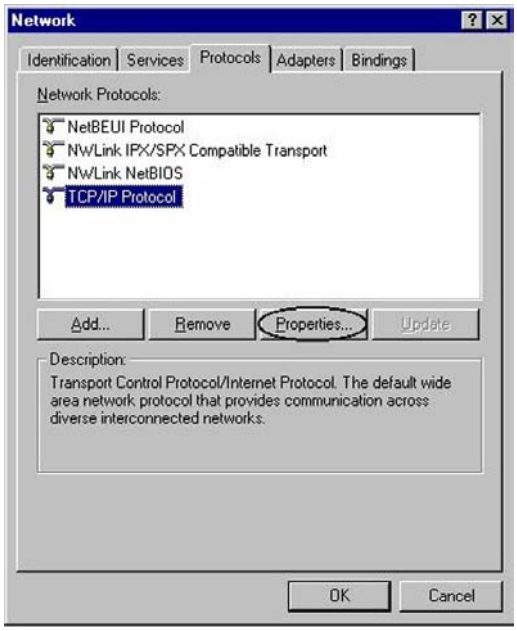


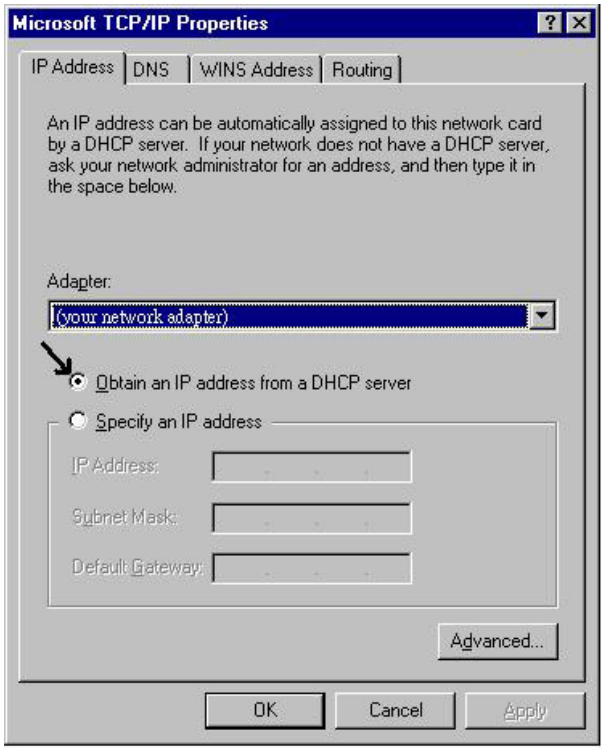
Configuration sous Windows NT4.0

1. Allez au **Panneau de Configuration**. Double-cliquez sur **Réseau** et enfin sélectionnez l'onglet **Protocole** .

2. Sélectionnez **TCP/IP Protocol** et après cliquez sur **Propriétés**.

3. Sélectionnez (votre carte Réseau) l'onglet **Obtenir une adresse IP par un serveur DHCP** et après cliquez sur **OK** pour terminer la configuration.

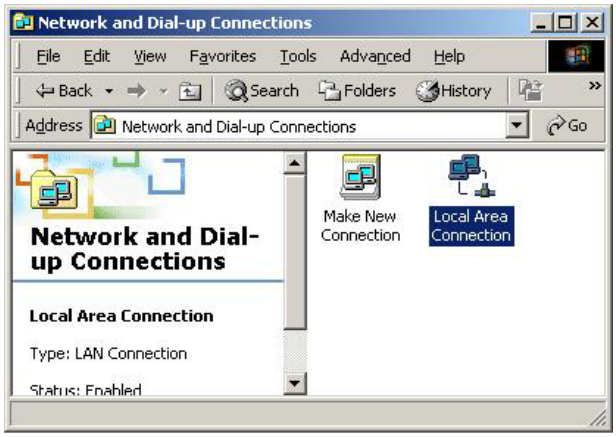



Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
(your network adapter)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

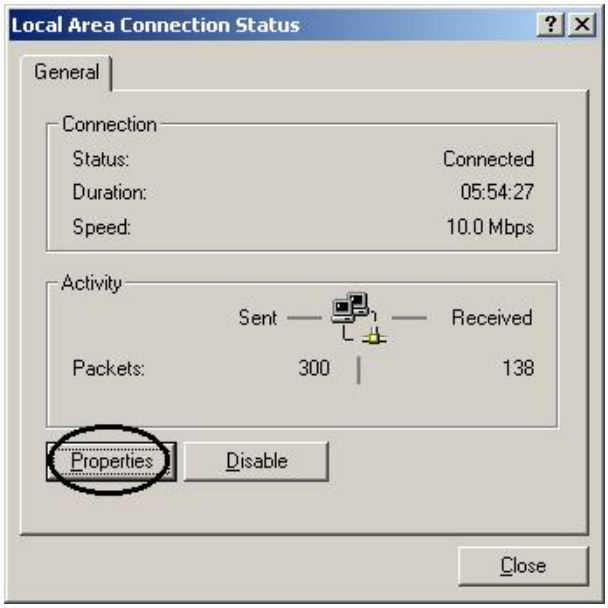
Configuration sous Windows 2000

1. Allez au **Panneau de Configuration**. Double-cliquez sur **Connexions Réseau et accès à distance.**.

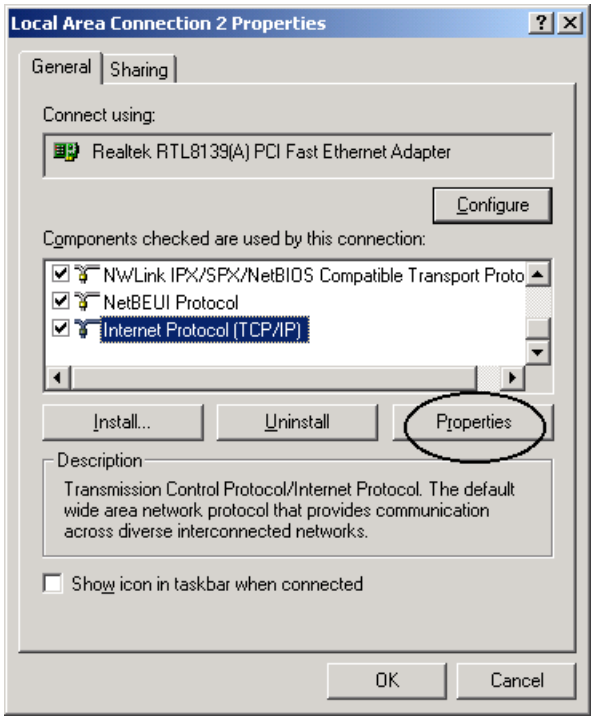
2. Double-cliquez sur **connexion au réseau local**.



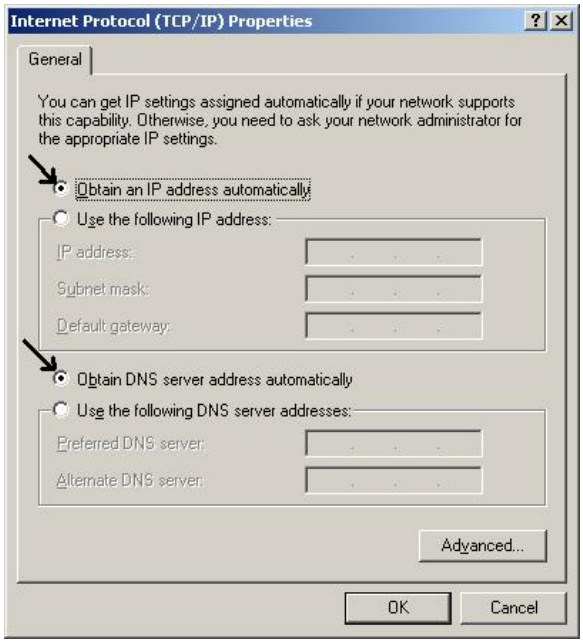
3. Dans **Connexion au réseau local** cliquez sur **Propriétés**.



4. Sélectionnez **Internet Protocol (TCP/IP)** et cliquez sur **Propriétés**.



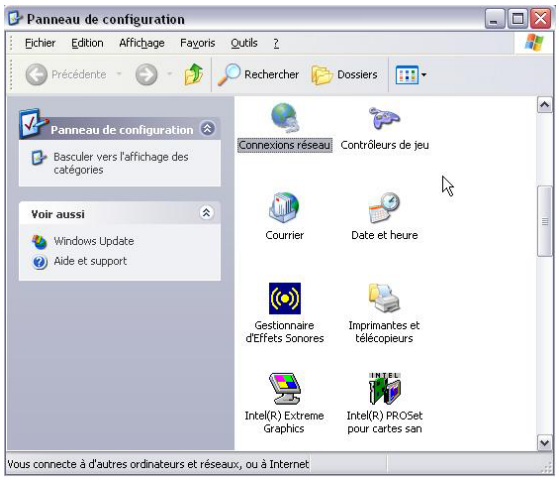
5. Sous l'onglet **Général**, sélectionnez l'onglet **Obtenir une adresse IP automatiquement** et après **Obtenir les adresses des serveurs DNS automatiquement**


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6. Cliquez sur **OK** pour terminer la configuration

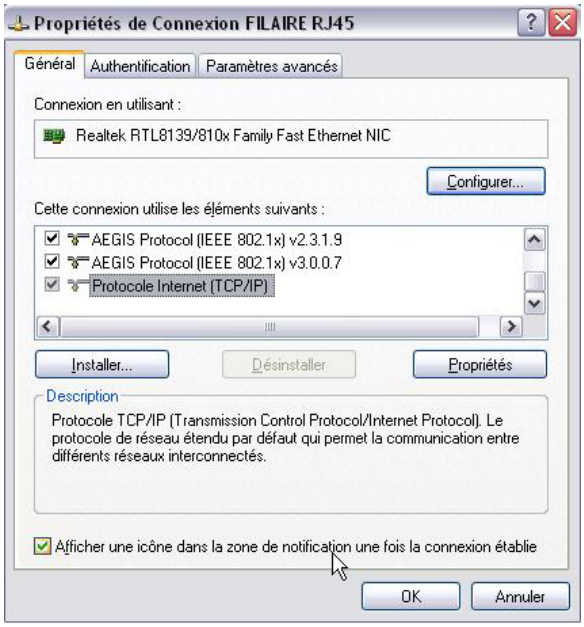
Configuration sous Windows XP

1. Allez sur **Panneau de Configuration**.
2. Double-cliquez sur **Connexions Réseau**.



3. Cliquez **Propriétés**.

4. Sélectionnez **Protocole Internet (TCP/IP)** puis cliquez sur **Propriétés**.


Propriétés de Connexion FILAIRE RJ45
Général
Authentification
Paramètres avancés
Connexion en utilisant :
Realtek RTL8139/810x Family Fast Ethernet NIC
Configurer...
Cette connexion utilise les éléments suivants :
AEGIS Protocol (IEEE 802.1x) v2.3.1.9
AEGIS Protocol (IEEE 802.1x) v3.0.0.7
Protocole Internet (TCP/IP)
Installer...
Désinstaller
Propriétés
Description
Protocole TCP/IP (Transmission Control Protocol/Internet Protocol). Le protocole de réseau étendu par défaut qui permet la communication entre différents réseaux interconnectés.
Afficher une icône dans la zone de notification une fois la connexion établie
OK
Annuler

5. Sélectionnez **Obtenir une adresse IP automatiquement** puis **Obtenir les adresses des serveurs DNS automatiquement**.

Propriétés de Protocole Internet (TCP/IP)
Général
Configuration alternative
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP :
Masque de sous-réseau :
Passerelle par défaut :
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré :
Serveur DNS auxiliaire :
Avancé...
OK
Annuler

6. Cliquez sur **OK** pour terminer la configuration.

3.3 Vérification

Pour vérifier le succès de la configuration (après avoir redémarré le PC pour Win98, SE, ME) utiliser la commande PING. Dans une fenêtre Dos écrivez: PING 192.168.1.254

Si le message suivant apparaît:

Pinging 192.168.1.254 with 32 bytes of date:
Reply from 192.168.1.254: bytes=32 times <10ms TTL=64
Reply from 192.168.1.254: bytes=32 times <10ms TTL=64
Reply from 192.168.1.254: bytes=32 times <10ms TTL=64
Reply from 192.168.1.254: bytes=32 times <10ms TTL=64

Vous pouvez continuer en allant au paragraphe suivant.
Si le message suivant apparaît par contre:

Pinging 192.168.1.254 with 32 bytes of date:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Vérifiez que la led LAN/WLAN est bien allumée.
Vérifiez l'adresse de votre PC en écrivant WINIPCFG (pour Win95, 98, ME) ou IPCONFIG (pour Win2000, XP) et éventuellement réinstallez le TCP/IP.
Maintenez la touche reset enfoncée pendant une dizaine de secondes. Le Wireless Routeur ADSL2+ fera un reboot et rechargera la configuration initiale.

3.4 Configuration initiale

Avant de commencer la configuration du Wireless Routeur ADSL2+ il est nécessaire d'en connaître la configuration initiale (paramètres par défaut).
Pour pouvoir utiliser le Wireless Routeur ADSL2+ rapidement, il suffit de garder la configuration par défaut, de mettre les PC en client DHCP et de configurer l'accès internet (avec les données fournies par le FAI).
La configuration initiale est:

- User : **admin**
- Password : **atlantis**
- Adresse IP (**192.168.1.254**), Subnet Mask (Masque de sous réseau)=**255.255.255.0**
- DHCP (Fonction **serveur DHCP**) Activée
- Wireless : SSSID = **wlan-ap**, Channel = **6**, WEP = **non activé**

3.4.1 Mot de Passe et Login

Il est conseillé de changer le password et le Login afin d'augmenter la sûreté.

Si vous ne vous rappelez plus de votre password il suffit de presser la touche reset pendant 10 secondes ou plus lorsque le routeur est allumé, jusqu'à la fin du clignotement des LED de faca avant puis redemarrer le routeur avec la touche Power On/Off.

3.4.2 Ports LAN et WAN

Les paramètres du Routeur sont pré-configurés. Les valeurs par défaut sont les suivantes :

Port LAN		Port WAN (FAI)
Addresse IP	192.168.1.254	N/A
Masque de sous réseau (Subnet Mask)	255.255.255.0	
Fonction serveur DHCP	Activée	

3.5 FAI

Avant d'installer votre Wireless Routeur ADSL2+, vous devez savoir de quel type d'accès Internet vous disposez et vous munir d'informations précises concernant votre compte. Si votre fournisseur d'accès demande un **Login** et un **Mot de Passe** (c'est parce que vous avez un compte **PPPoE** ou **PPPoA**, par exemple), utilisez le protocole **PPPoA (RFC2364)** ou **PPPoE (RFC2516).** Si vous avez une adresse IP fixe utilisez le protocole **RFC 1483 Routed** ou **RFC1577**. Le FAI, dans ce cas, doit vous fournir aussi: Adresse IP Internet, Masque de sous-réseau, Adresse IP de la passerelle par defaut et Adresse(s) IP du serveur DNS. Le tableau suivant récapitule les informations dont vous aurez besoin en fonction du protocole:

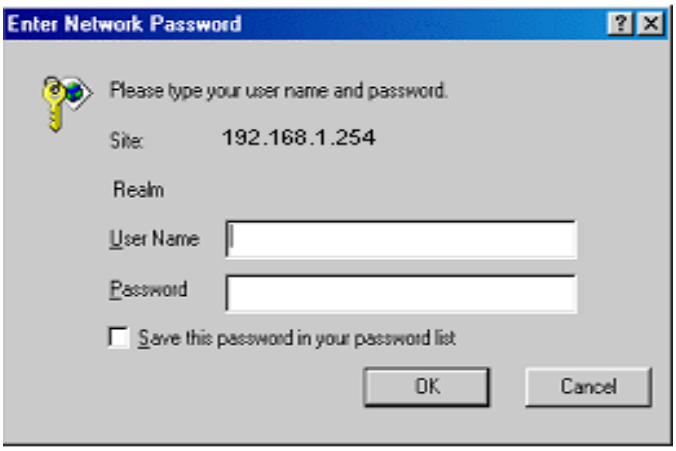
PPPoE	VPI et VCI Multiplexage VC ou LLC Nom d'utilisateur et Mot de passe Nom du Service
PPPoA	VPI et VCI Multiplexage VC ou LLC Nom d'utilisateur et Mot de passe
RFC1483 Bridged	VPI/VCI Multiplexage VC ou LLC
RFC1483 Routed	VPI/VCI Multiplexage VC ou LLC Adresse IP Masque de sous-réseau Adresse IP de la passerelle par défaut Adresses IP des serveurs DNS
IPoA	VPI/VCI Multiplexage VC ou LLC Adresse IP Masque de sous-réseau Adresse IP de la passerelle par défaut Adresses IP des serveurs DNS

3.6 Configuration avec le Navigateur

Pour accéder à l'interface Web, lancez un navigateur Internet et tapez dans la barre d'adresse, l'IP suivante :

http://192.168.1.254

Un mot de passe vous est demandé, pour la première connexion.
User Name= **admin**
Password = **atlantis**
et appuyez sur **OK** pour entrer dans la configuration.



Il faut sauver la configuration au fur et à mesure, en cliquant sur la section **Save Config to Flash**, afin d'enregistrer chaque modification.

Nous accédons au Menu Principal avec les sections suivantes:

- **Status (ARP Table, Routing Table, DHCP Table, System Log, Security Log)**
- **Quick Start**
- **Configuration (WAN, LAN, System, Firewall, QoS, Virtual Server, Advanced)**
- **Save Config to Flash**

3.6.1 STATUT (STATUS)

Dans cette section, on visualise l'ensemble des états du Routeur par un tableau récapitulatif. En cliquant sur le Menu **Status**, les sous-sections suivantes s'ouvriront :

- **ARP Table**
- **Routing Table**
- **DHCP Table**
- **System Log**
- **Security Log**

3.6.1.1 Table ARP

La table ARP (Address Resolution Protocol) montre les liaisons existantes entre les adresses IP et les adresses MAC. C'est la solution la plus simple pour connaître l'adresse MAC d'un des PCs de votre réseau afin de régler (si vous le souhaitez) la fonction de filtrage **Firewall – MAC Address Filter**. Voir la section Firewall pour de plus amples détails.

Table ARP

List IP <> MAC

Adresse IP	Adresse MAC	Interface	Statique
192.168.1.185	00:E0:18:DF:7B:64	iplan	Non
192.168.1.101	00:0D:93:64:98:22	iplan	Non

- **Adresse IP(IP Address):** Liste des Adresses IP des péripheriques de votre réseau.
- **Adresse MAC(MAC Address):** Liste des Adresses MAC des péripheriques de votre réseau.
- **Interface**: Le nom de l'interface du routeur sur laquelle cette adresse IP est connectée.
- **Statique(Static)**: Pour le Statut de l'adresse IP:
- **Non(no)** allocation dynamique
- **Oui(yes)** allocation manuelle par l'utilisateur

3.6.1.2 Table de Routage

Pour visualiser et créer les routages du A02-RA241-W54.

Table de routage

Table de routage

#	Destination	Masque de sous réseau	Passerelle/Interface	Coût		
1	85.40.14.212	255.255.255.252	0.0.0.0/ipwan	0	Editer	Supprimer
2	192.168.1.0	255.255.255.0	0.0.0.0/iplan	0	Editer	Supprimer
3	0.0.0.0	0.0.0.0	85.40.14.213/ipwan	0	Editer	Supprimer

Créer

Route statique

Ajouter une règle4

Destination			
Masque de sous réseau			
Passerelle		Interface	Merci de sélectionner
Coût	0		

Appliquer Abandon

- #: **Numéro**
- **Destination:** L'adresse IP du réseau de destination.
- **Masque de sous réseau(Netmask):** Le masque de sous réseau.
- **Passerelle/Interface(Gateway/Interface)**: L'adresse IP de la passerelle ou de l'interface utilisée.
- **Cout(Cost):** Valeur non obligatoire dans la plage 0 à 65535.
- **Interface:** L'interface utilisée pour la transmission des paquets de données.

3.6.1.3 Table DHCP

Table DHCP

Table de durée de bail

Adresse IP	Adresse MAC	Nom de Client	Temps
192.168.1.100	00:e0:18:df:7b:64	Tolomeo	2005/07/18 14:56:24 - 2005/07/19 02:56:24
192.168.1.101	00:0d:93:64:98:22	mac-mini-di-dimitri-pescatori	2005/07/18 16:07:30 - 2005/07/19 04:07:30

- **Adresse IP(IP Address):** L'adresse IP de votre ordinateur ou périphérique.
- **Adresse MAC(MAC Address):** L'adresse MAC de la carte réseau de votre ordinateur ou périphérique
- **Nom de Client(Client Host Name):** Le nom de votre ordinateur
- **Temps(Register Time):** La durée de vos droits DHCP

3.6.1.4 Evénement Système

Pour visualiser les événements système.

Evénements système

Temps actuel:Mon Jul 18 16:31:47 2005

Si vous voulez sauvegarder au format .txt, click droit here puis sélectionner \"Save Target As ...\"

```
Jan  1 00:00:05 syslog: OS (13:19:45, Jul 15 2005)
Jan  1 00:00:05 syslog: 199.47 MIPS
Jan  1 00:00:05 syslog:
============================================================
Jan  1 00:00:05 syslog: TC3162 PCI interface initialize
Jan  1 00:00:05 syslog: Initializing RT netlink socket
Jan  1 00:00:05 syslog: wdt_init ..
Jan  1 00:00:05 syslog: TC3162 wtachdog initialize at Interrupt 9
Jan  1 00:00:05 syslog: ADSL DMT initialization starting
```

Rafraichir | Effacer

3.6.1.5 Evénements de Sécurité

Pour visualiser les événements de Sécurité, par exemple lorsque qu'une attaque de « hacker » est bloquée par le Firewall du routeur, une ligne d'information est génerée et vous pouvez trouver les renseignements relatifs à cette attaque.

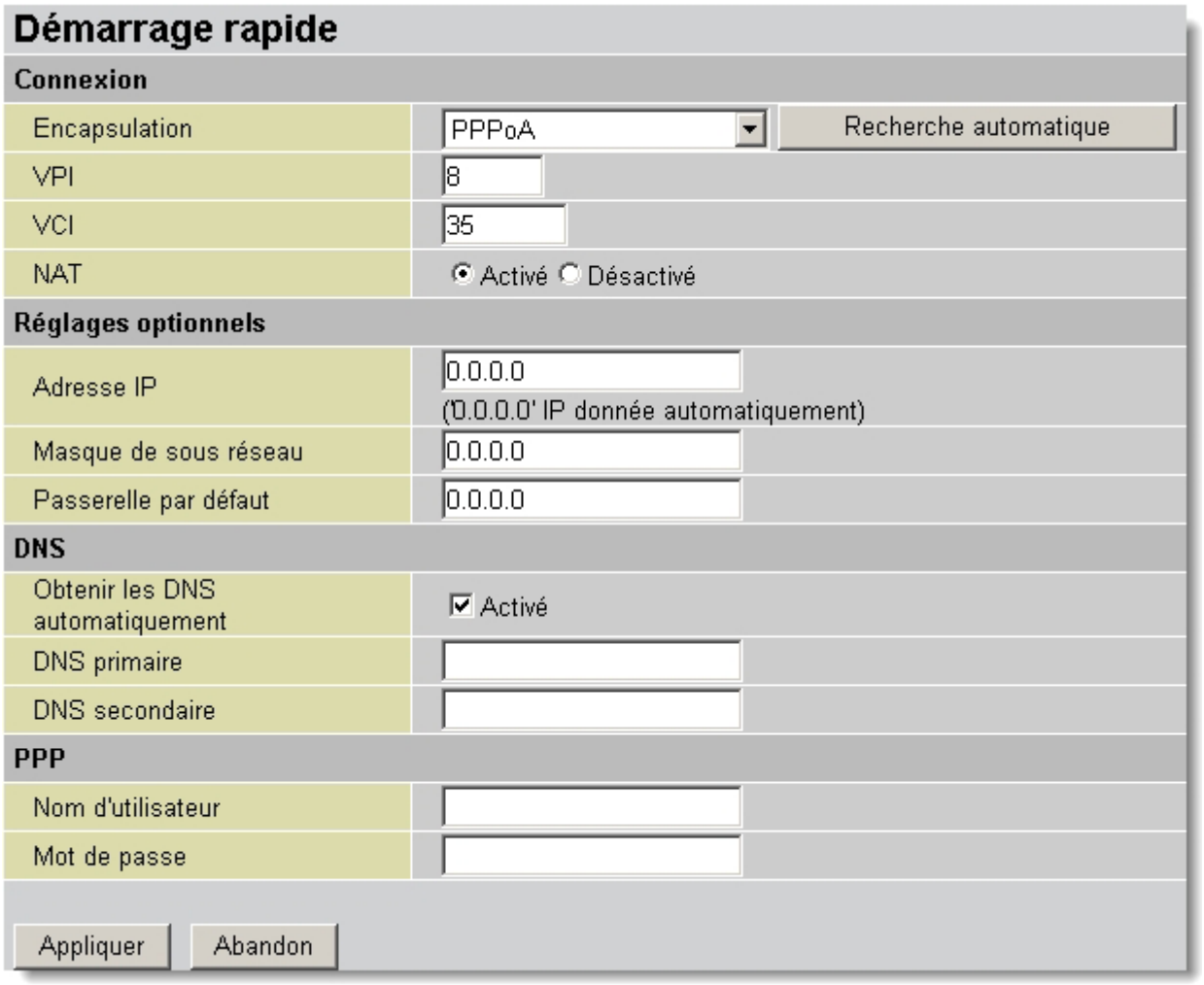
Evénements de sécurité
Temps actuel:Mon Jul 18 16:32:18 2005
Si vous voulez sauvegarder au format .txt, click droit here puis sélectionner \"Save Target As ...\"
Rafraichir
Effacer

3.6.2 Guide d'installation rapide

Pour les informations détaillées de configuration WAN, consultez la section WAN de ce manuel.

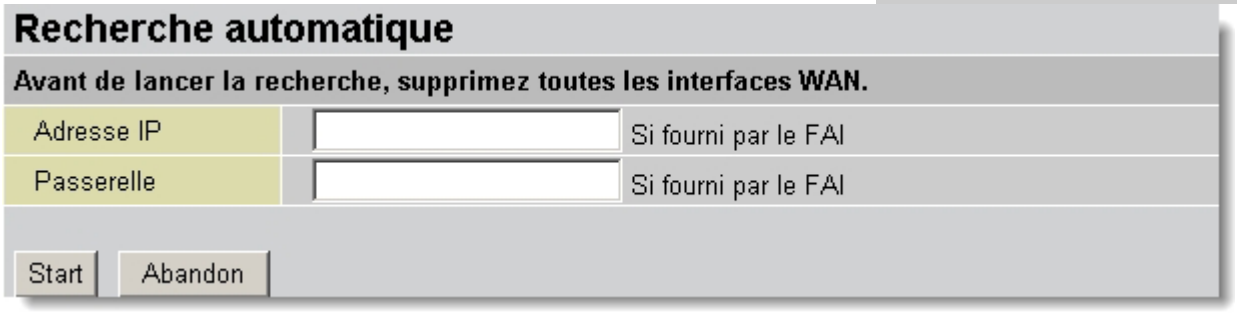
Les informations nécessaires pour configurer votre connexion avec l'Assistant Rapide sont votre « login » (format répandu : username@ispname), votre mot de passe et le type d'encapsulation.

Votre FAI (Fournisseur d'Accès Internet) peut vous communiquer tous les renseignements nécessaires. Vous pouvez aussi utiliser la fonction d'Auto Scan permettant de determiner automatiquement le type d'encapsulation utilisée par votre FAI.



Connexion

Encapsulation: Pour le type d'encapsulation ou par l'"**Recherche Automatique** (**Auto Scan)**".



Cliquez sur **Start** pour lancer l'Auto Scan.

- **VCI:** Pour le VCI de votre connexion. Ce champ peut être déjà rempli.
- **VPI:** Pour le VPI de votre connexion. Ce champ peut être déjà rempli.
- **NAT:** Sélectionnez "**Activé(Enabled)**".

Paramètres Optionnels

- **Adresse IP(IP Address):** Si vous avez une adresse IP fixe (fournie par votre FAI).
- **Mask de Sous Réseau(Subnet Mask):** Pour le masque de sous réseau (adresse fournie par votre FAI).
- **Passarelle par Défaut(Default Gateway):** Pour la passerelle par défaut (adresse fournie par votre FAI).

DNS

- **Obtenir le DNS automatiquement (Obtain DNS automatically):** Case à cocher pour obtenir automatiquement les adresses des serveurs de DNS de votre FAI.
- **DNS Primaire(Primary DNS):** Adresse IP du Serveur primaire de DNS. Données transmises aux clients DHCP.
- **DNS Secondaire(Secondary DNS):** Adresse IP du Serveur secondaire de DNS. Données transmises aux clients DHCP.

PPP

- **Nom d'utilisateur(Username):** Pour le nom d'utilisateur fourni par votre FAI.
- **Mot de passe(Password):** Pour le mot de passe fourni par votre FAI

Cliquez sur **Appliquer(Apply)** puis sur **Save Config.**

3.6.3 CONFIGURATION

En cliquant sur **Configuration,** les sous-sections suivantes apparaitront:

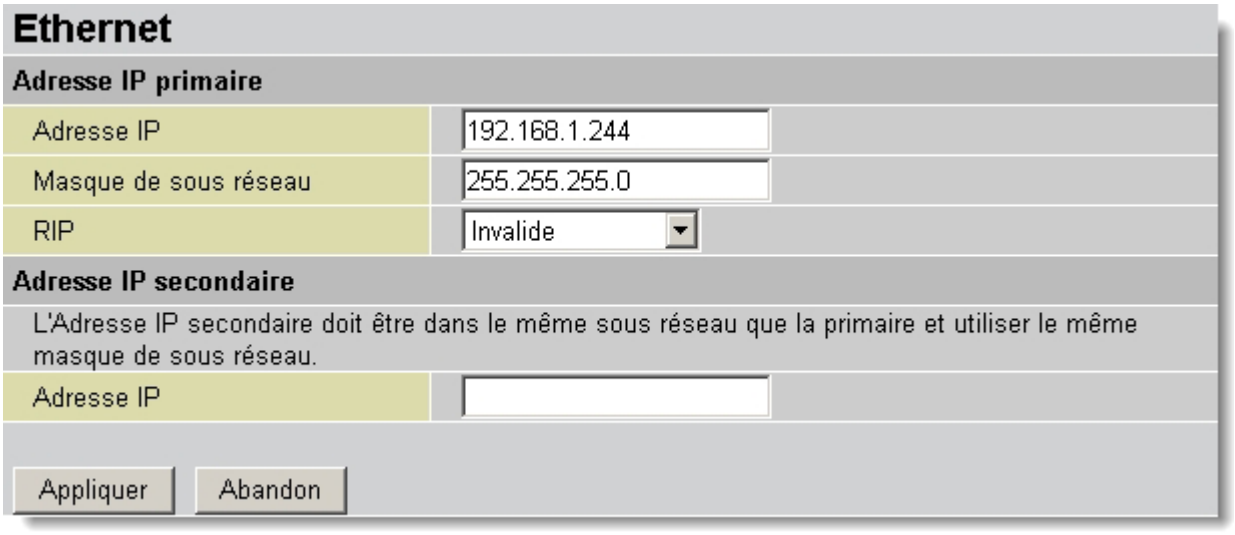
- **LAN**
- **WAN**
- **System**
- **Pare Feu (Firewall)**
- **QoS**
- **Serveur Virtuel (Virtual Server)**
- **Avancé (Advanced)**

3.6.3.1 LAN

Voyons les choix de la sous-section LAN.
En cliquant sur **LAN,** les sous-sections suivantes apparaitront:

- **Ethernet**
- **Wireless**
- **Wireless Security**
- **DHCP Server**

3.6.3.1.1 Ethernet

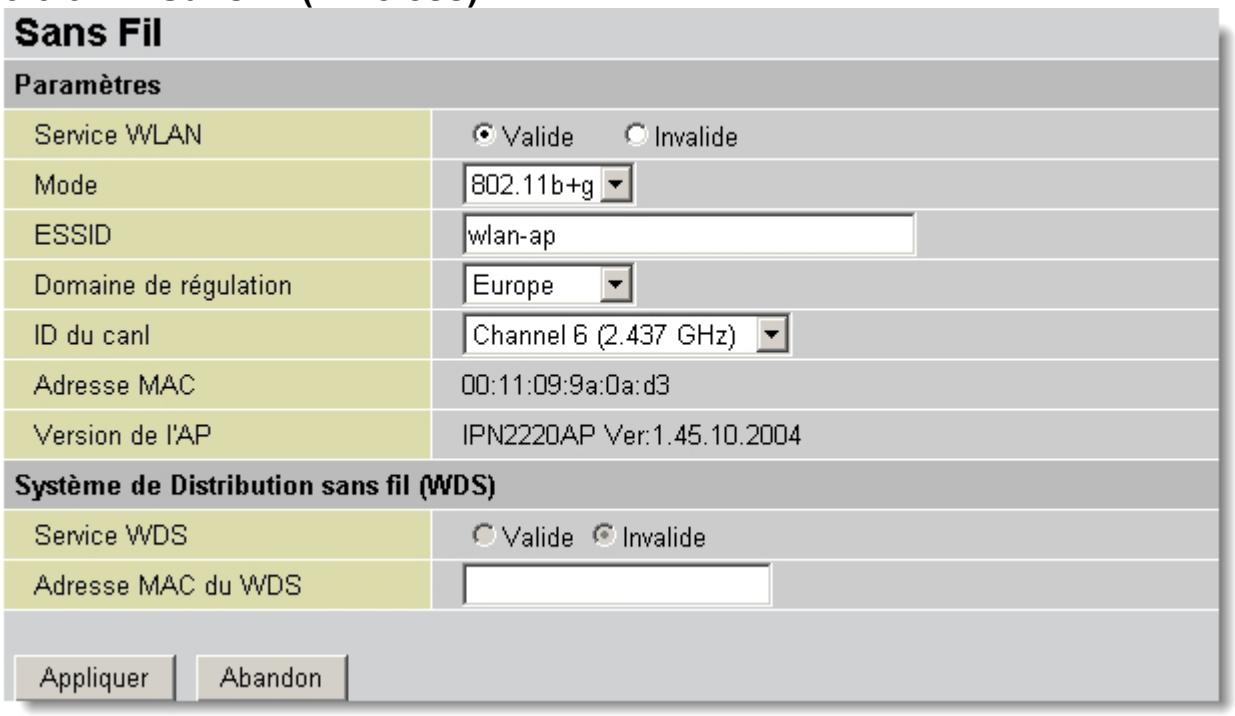


Dans cet écran, vous pouvez changer l'adresse IP du routeur sur le réseau local. L'adresse par défaut est 192.168.1.254 (si cette adresse existe déjà sur votre réseau, vous ne pourrez pas accéder au routeur).

RIP: RIP v1, RIP v2, RIP v1+v2 et RIP v2 Multicast.

Le masque de sous réseau de l'adresse IP secondaire est le même que pour le primaire.

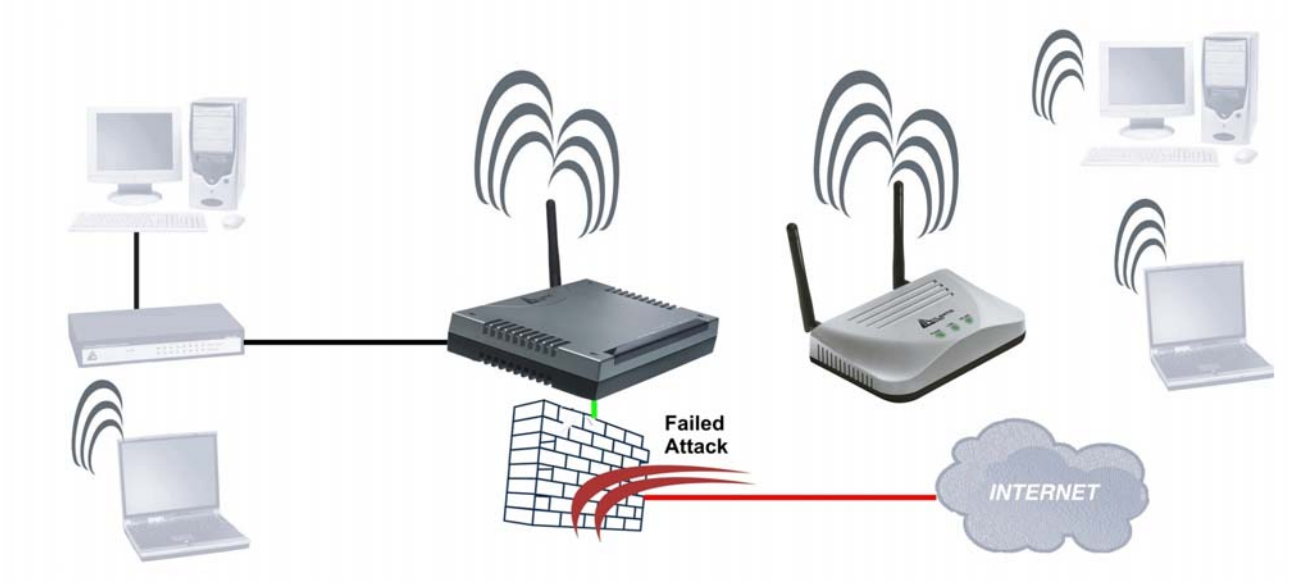
3.6.3.1.2 Sans Fil(Wireless)



Service WLAN(WLAN Service) : Pour activer/ désactiver la section sans fil
Mode : Pour sélectionner le type de bande utilisée (mode mixte, uniquement G ou B).

- ***Mixed mode:*** Pour utiliser simultanément des appareils en 802.11g et 802.11b.
- ***G-only:*** Pour n'utiliser que des appareils en 802.11g.
- ***B-only***: Pour n'utiliser que des appareils en 802.11b.

ESSID: Entrer le nom que vous voulez donner à votre réseau sans fil. Les clients doivent utiliser le même pour pouvoir se connecter.
Demain de règulation(Regulation Domain) : Chaque pays utilise des bandes de fréquences fixées par un organisme féderateur, l'utilisateur final doit s'assurer du bon choix de canal par rapport au pays d'utilisation.
ID du canal(Channel ID): Sélectionner le Canal ID que vous voulez utiliser,14 canaux sont disponibles et définis pays par pays, sélectionnez en un parmi ceux autorisés dans votre région.
Address MAC(MAC Address): L'adresse MAC du routeur.
Version de l'AP(AP Version): La version du firmware.
Service WDS(WDS Service) : WDS (Wireless Distribution System) utilise le Wireless pour relier des appareils entre eux. Permet d'étendre le rayon de couverture d'un réseau wireless. Introduisez le MAC du routeur dont on souhaite étendre la couverture. Les deux appareils du lien WDS doivent avoir la même configuration (Canal, WEP, SSID). Exemple typique de montage ci-après.



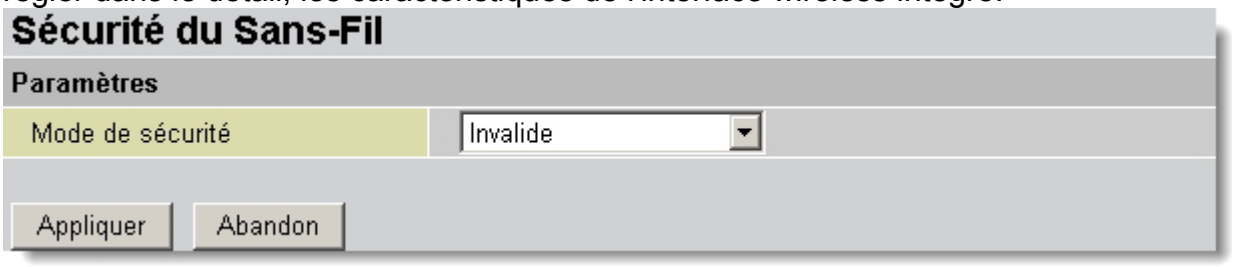
La plage de fréquences radio utilisées par les appareils Wireless IEEE 802.11g, est partagée en “canaux”. Le nombre de canaux disponibles dépend de la zone géographique d’appartenance. Sélectionnez des canaux différents pour éliminer d’éventuelles interférences avec des Points Access proches. L’interférence se vérifie quand deux ou plusieurs canaux s’interposent en dégradant les performances, c’est l’“Overlap”.
On conseille de maintenir une plage de 5 canaux entre deux utilisés (ex. AP1-canal 1, AP2-canal 6).

L’utilisateur final doit donc s’assurer du bon réglage de son AP sur un canal autorisé dans son pays.

Pour un bon fonctionnement, vérifiez que vos différents APs soient bien sur le même canal, avec le même SSID et utilisent la même clé WEP.
Seul le cryptage WEP est utilisable quand le WDS est actif.

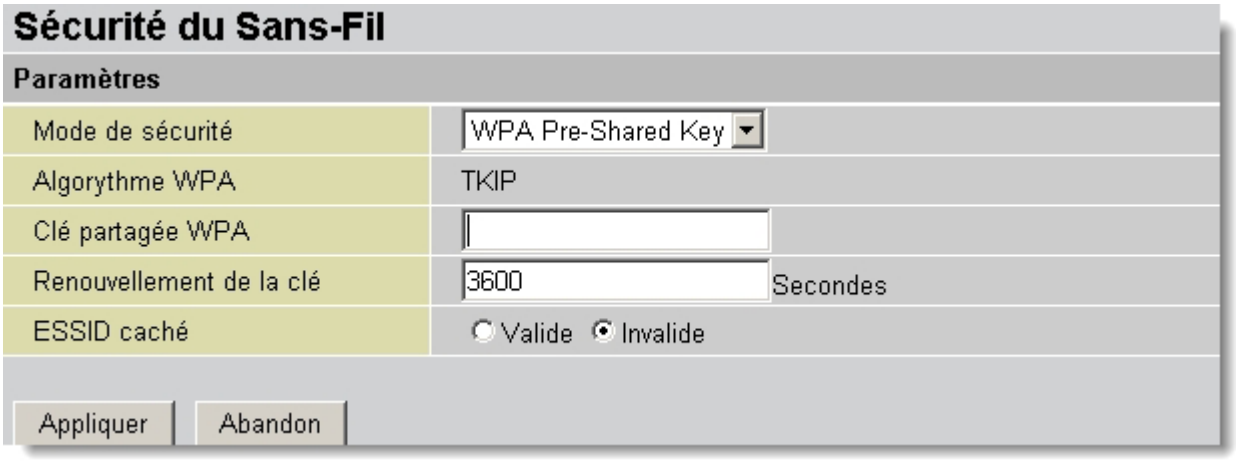
3.6.3.1.3 Sécurité du Sans-Fil(Wireless Security)

Dans la section **Sécurité du Sans-Fil(Advanced Wireless Configuration,** vous pouvez régler dans le détail, les caractéristiques de l'interface wireless intégré.



WPA Pre-Shared Key:

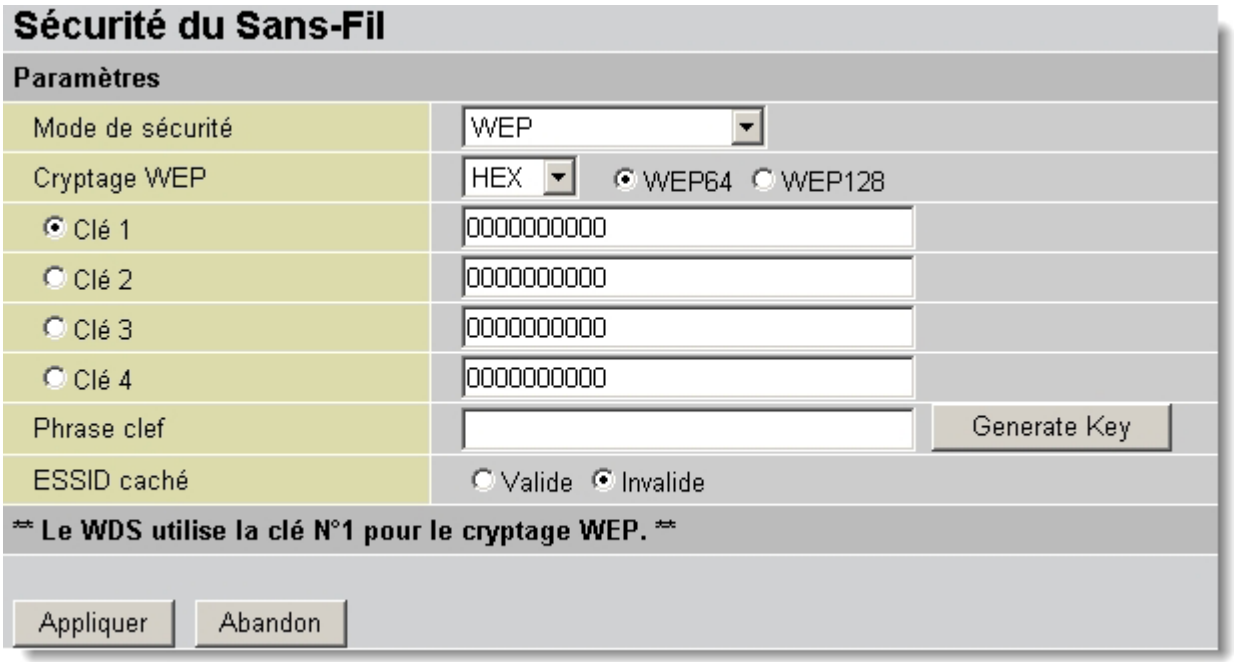
Choisir **WPA Pre-Shared Key** pour activer la modalité WPA.



- **WPA Algorithms:** TKIP (Temporal Key Integrity Protocol) utilise un cryptage plus important et incorpore Message Integrity Code (MIC) pour se protéger des hackers**.**
- **Clé Partagée WPA (WPA Shared Key):** La clé pour l'authentification réseau. Le format est de type caractère et la taille est comprise entre 8 et 63.
- **Renouvellement Automatique de Clé (Group Key Renewal):** Période avant le changement automatique de la clé entre les clients et l'Acces Point (AP).
- **ESSID caché(Hide ESSID):** Pour partager le SSID de l'AP, si cette fonction est selectionée, les stations doivent le connaître par avance.

WEP:

Choisir **WEP** pour activer la modalité WEP.

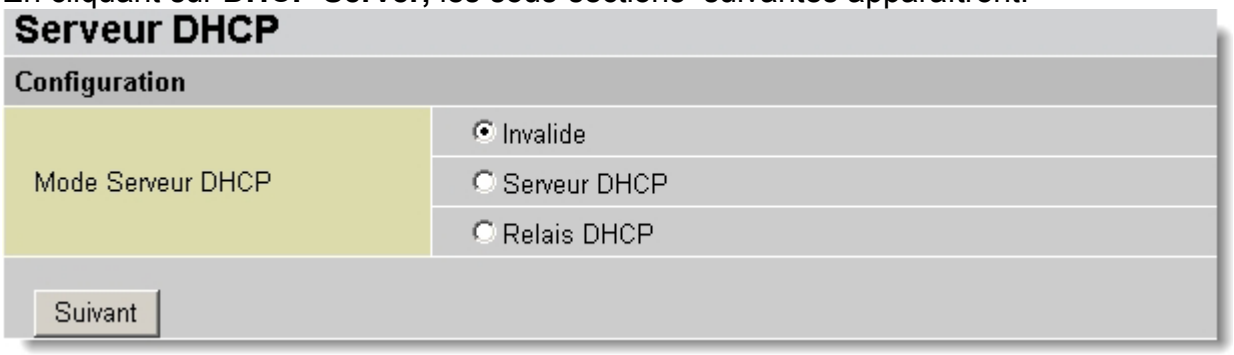


- **Cryptage WEP (WEP Encryption):** Pour protéger l'accès des données transmises sur le réseau sans fil, le routeur permet de crypter les données selon le standard WEP. Il existe deux niveaux de cryptage, WEP 64 et WEP 128. WEP 128 offre une sécurité accrue par rapport au WEP 64.

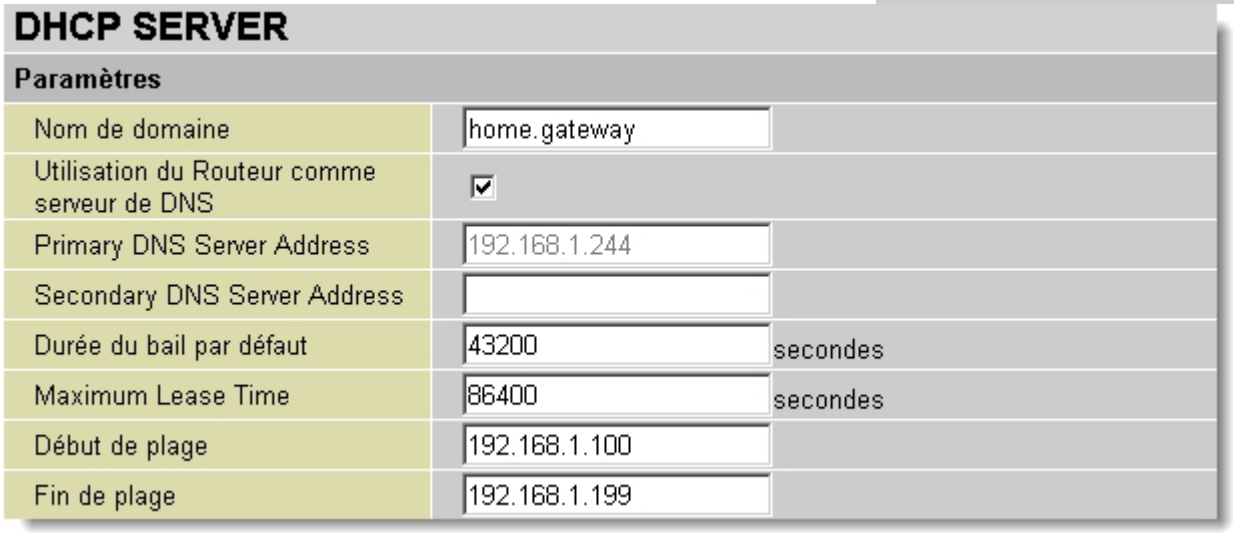
- **Phrase Clef (Passphrase):** Utilisée pour générer automatiquement une clé à partir de cette valeur, en utilisant l'algorithme de WEP 64 ou WEP 128. Vous devez utiliser la même phrase dans les cartes clients pour générer une clé compatible. Il ne faut pas entrer de clé (1-4), si la fonction Phrase Clef est utilisée.
- **WEP Clé par défaut:** Pour sélectionner la clé de cryptage, suivez les renseignements ci-dessous. Clé (1-4): Entrer la clé pour crypter les données du réseau sans fil, pour que l'intégralité des stations du réseau soit protégée, il faut utiliser la même clé que celle du routeur. Il y a quatre clés pour la sélection, le format est en Hex, code 5 ou 13, sans séparateur. Exemple, en WEP64 1122334455 est valide, 11-22-33-44-55 ne l'est pas.
- **ESSID Caché(Hide ESSID):** Pour partager le SSID, si cette fonction est selectionnée, les stations doivent le connaître par avance.

3.6.3.1.4 Serveur DHCP

En cliquant sur **DHCP Server,** les sous-sections suivantes apparaîtront:



- **Invalide (Disable):** Le serveur DHCP est désactivé, vous devez attribuer manuellement une adresse IP à chaque PC du réseau.
- **Serveur DHCP (DHCP Server):** Cette fonction vous permet de profiter des avantages de la fonction **DHCP**, qui attribue dynamiquement des adresses IP aux machines de votre réseau local. Il suffit de mettre le premiere et le derniere adresse IP. Laisser **DHCP Gateway Selection=Automatic.**
- **Relais DHCP(DHCP Relay):** Vous devez attribuer manuellement une adresse IP au serveur DHCP (qui n'est pas dans votre réseau).



Pour configurer le serveur DHCP du routeur, cochez **Serveur DHCP(DHCP Server)** puis cliquez sur **Suivant(Next)**. Vous pouvez maintenant entrer les paramètres du serveur DHCP, la plage d'adresse IP (adresses de départ et de fin qui seront automatiquement attribuées aux ordinateurs de votre réseau local), le temps ou l'adresse IP sera valide, les adresses IP des serveurs de DNS. Ces renseignements sont fournis aux clients DHCP (par exemple votre PC) lorsqu'ils demandent une adresse IP au serveur. Cliquez sur **Appliquer (Apply)** pour mettre en route cette fonction. Si vous cochez " **Utilisation du Routeur comme serveur de DNS (Use Router as a DNS Server)**", le routeur distribuera le nom de domaine, en trouvant à l'exterieur son adresse IP,aux PC du réseau qui en feront la demande.

3.6.3.2 WAN

Il existe plusieurs modalités pour la connexion avec le FAI: **PPPoE, PPPoA, RFC1483 routed et RFC1483 Bridge**.

- **VPI/VCI:**

Données à configurer	**Valeurs**		
Virtual Path Identifier	8	8	2
Virtual Circuit Identifier	67	35	32
Framing	LLC/VC-Mux		

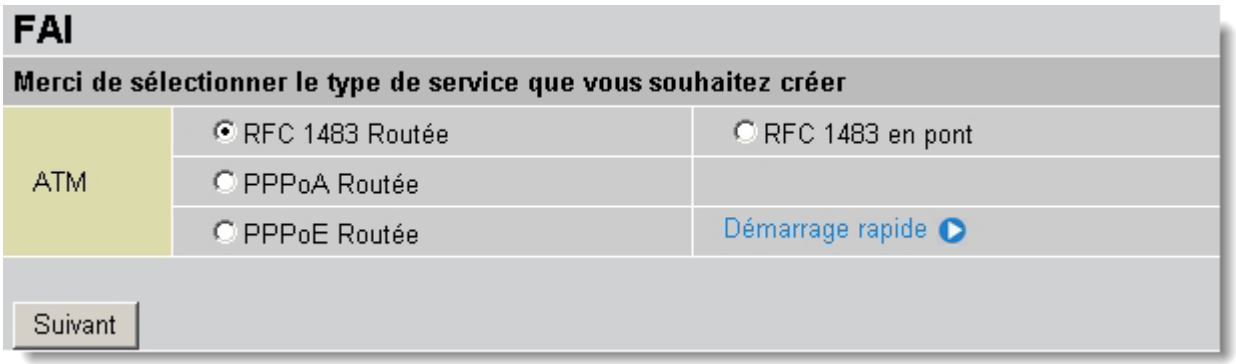
- **NAT:** (Network Address Translation) permet de convertir une adresse IP interne en adresse IP externe. Cette fonction doit être activée si vous voulez pouvoir partager votre accès Internet.
- **Encapsulation Method:** Choisir entre LLC/SNAP ou VC MUX.

En cas de doute, demandez confirmation à votre fournisseur d'accès.
En choisissant la section Configuration **puis la sous-section** WAN **vous pouvez régler la configuration pour la liaison avec le FAI.**

Voyons les choix de la sous-section WAN.
En cliquant sur **WAN,** les sous-sections suivantes apparaitront:
ISP
DNS
ADSL

3.6.3.2.1 ISP

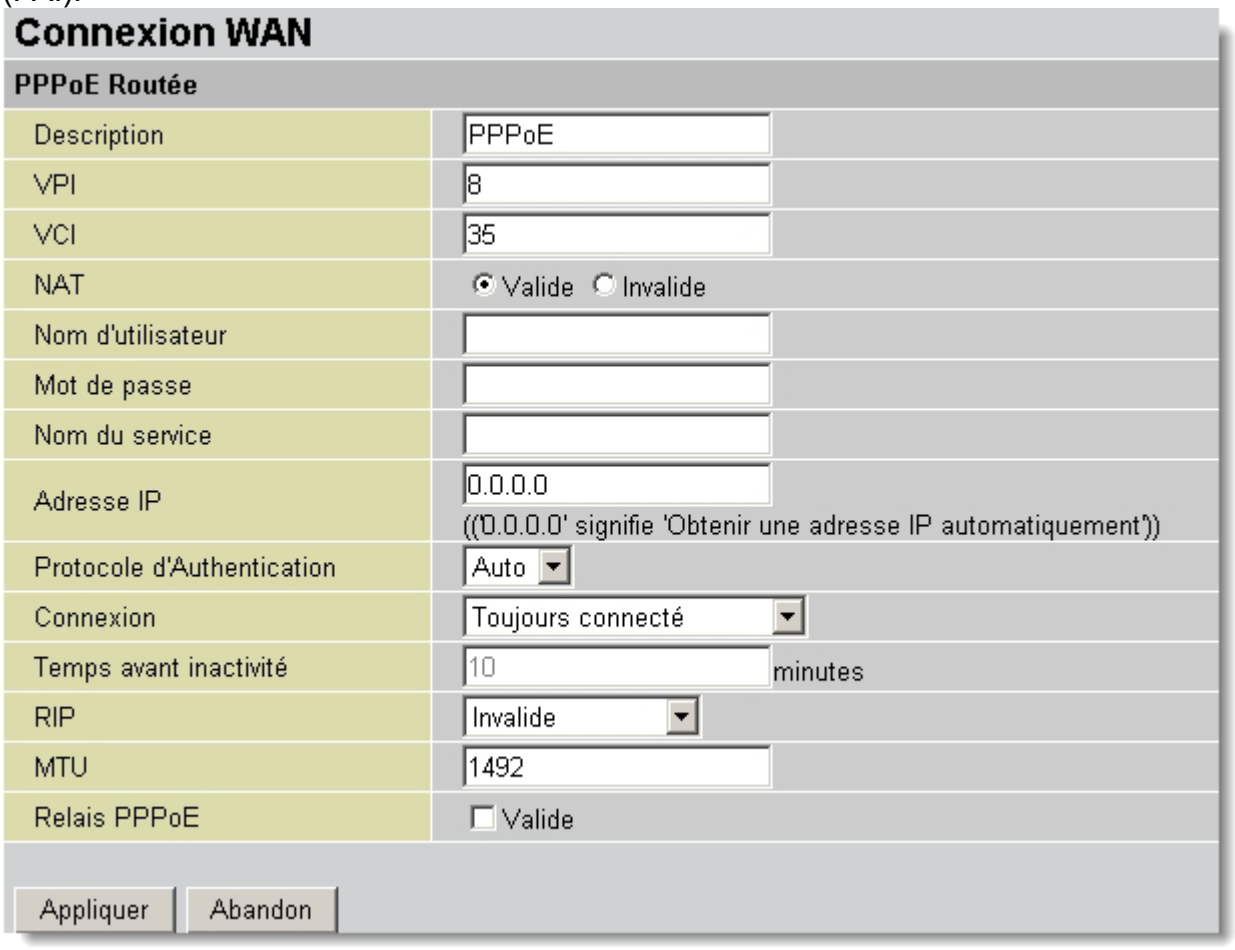
La valeur par défaut est PPPoE. Si votre FAI utilise ce protocole, cliquez sur **Changer(Edit)** pour renseigner les autres paramètres, sinon vous pouvez changer les paramètres par défaut.
Une alternative simplifiée existe en cliquant sur **Démarrage Rapide (Quick Start),** consultez la section Quick Start du manuel pour de plus amples informations.



Cliquez su **Suivant(Next)** pour valider la configuration.

PPPoE (RFC 2516) ou PPPoA (RFC 2364)

Conçus pour compléter le service ADSL avec une attention particulière à la simplicité de configuration. L'utilisateur peut bénéficier d'une grande vitesse d'accès et partager avec tous les utilisateurs du réseau, un compte Internet unique. Il ne faut pas utiliser de logiciel additionnel. En cas de doute, demander les paramètres de configuration à votre opérateur (FAI).



- **Description:** le type connexion.
- **VPI/VCI: demander les paramètres de configuration à votre opérateur (FAI).**
  - **VPI = 8, 8, 2**
  - **VCI = 67, 35, 32**
- **NAT:** choisir **Valide(Enable).**
- **Nom d'utilisateur(Username):** Nom d'utilisateur (maximum 63 caractères alphanumériques).
- **Mot de Passe(Password):** Mot de passe (maximums 63 caractères alphanumériques).
- **Nom du Service (Service Name):** Identificateur qui peut être demandé par le FAI**.** Uniquement en PPPoE.
- **Adresse IP(IP Address):** Laisser 0.0.0.0
- **Protocole d'Authentication (Authentication Protocol):** (Méthode d'authentification de l'utilisateur : Auto – PAP – CHAP). Ce choix dépend de votre FAI, laisser par défaut sur Auto, le routeur Wirelesss se chargera du choix en fonction de la ligne.
- **Connexion(Connection):** Il faut choisir entre **Toujours connecté** (Always On) et **Connection à la demande** (Connect on Demand)**.** Seulement en PPPoE.

- **Toujours connecté(Always on):** Cochez cette option si vous désirez que votre connexion ADSL soit toujours active.
- **Connection à la demande(Connect on Demand)** Pour une connexion automatique lorsqu'un logiciel en fait la demande (Navigateur, Messagerie, etc…). **Uniquement en PPPoE.**

- **Temps avant inactivité (Idle Timeout):** Réglage du temps, compté en minutes, précédant la déconnexion automatique. En mettant zéro, cette fonction ne sera pas activée.
- **RIP:** RIP v1, RIP v2, RIP v1+v2 et RIP v2 Multicast.
- **MTU:** Laisser les valeurs par défaut. Il faut utiliser 1492 (PPPoE),1500 (PPPoA).

En cliquant sur **Appliquer(Apply)**, le Wireless Routeur ADSL2+ fera un reboot automatique. Lorsque la session PPPoE/PPPoA est connectée,les LEDs **ADSL et PPP sont Allumées en fixe et** votre PC est prêt pour la navigation.Cliquez sur **Sauvegarde en mémoire** (**Save Config) to Flash** pour terminer et enregistrer vos paramètres de réglages.

Rappel : les Routeurs ne sont pas aptes à gérer les abonnements à la consommation.

Nat signifie Network Address Translation (translation des adresses du réseau local). Il a été proposé et décrit dans l'RFC-1631 et il avait, au moins au début, la tâche de permettre une exploitation intensive des adresses IP. Chaque appareil supportant le NAT est composé d'un tableau basé sur des couples d'adresse IP (privée et publique). Le Router Wireless ADSL supporte le NAT, plusieurs utilisateurs peuvent accéder à Internet en utilisant un seul compte (et une seule IP publique). Si les utilisateurs du réseau ont des adresses IP publiques et peuvent donc accéder directement à Internet, cette fonction doit être désactivée. Le Nat agit comme premier pare-feu en améliorant la sécurité du réseau local. Cette fonction n'entre pas en conflit avec les fonctions Virtual Server, DMZ et DHCP. Le Nat manipule les paquets IP sortants et il change le champ **IP expéditeur** (dans ce cas l'adresse IP de l'ordinateur qui est une IP privée non valide Internet) avec l'IP publique du Wireless ADSL Router. De cette façon tous les paquets sortants du Router auront dans le champ expéditeur l'adresse IP publique du Router. Puis, quand les paquets reviennent au Router, grâce aux tableaux sauvegardés, ils pourront être renvoyés à l'ordinateur émetteur.

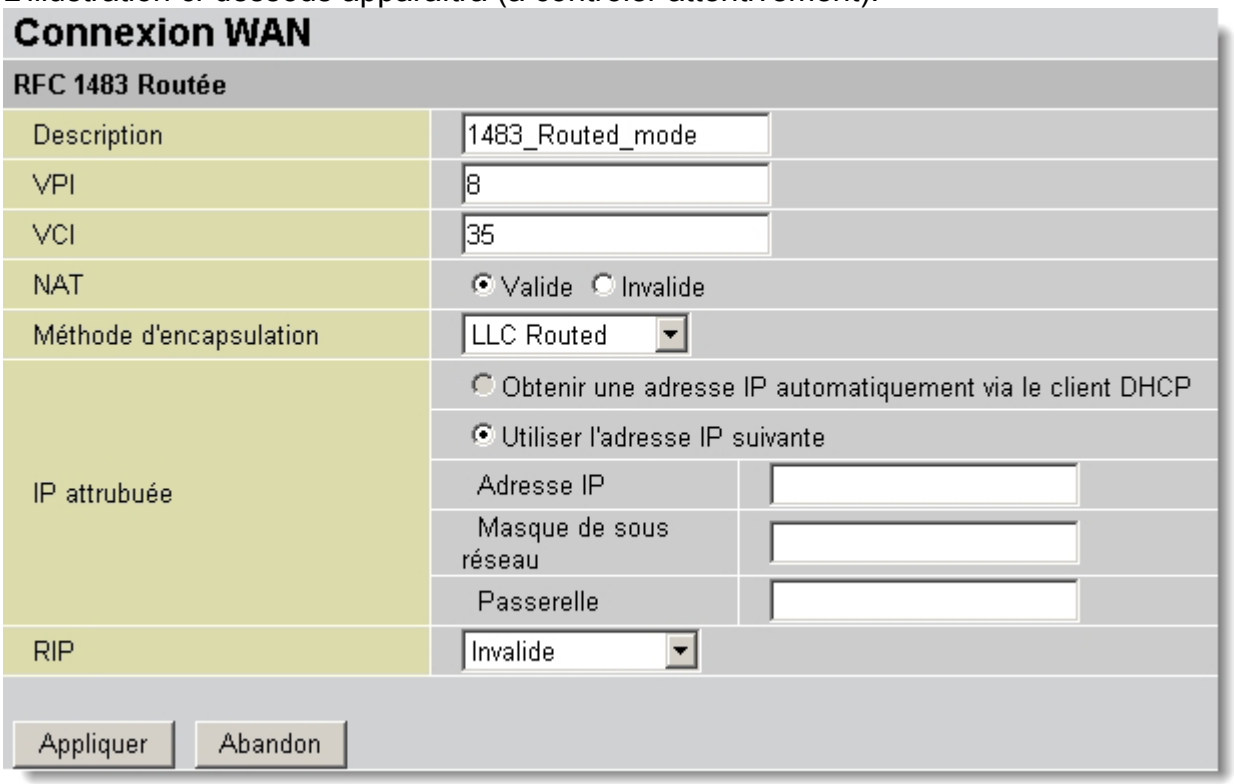
RFC 1483 Routing

Les modalités d'utilisation pour lesquelles le FAI peut fournir RFC1483 sont les suivantes :

1. **Un adresse IP publique statique**. Dans ce cas il faudra configurer la section WAN-ISP comme suit : NAT= habilité et IP address = adresse IP publique et statique assignées, Subnet mask et Default Gateway (qui sera une adresse IP publique) seront fournies par le FAI. Le LAN-IP sera au contraire dans une typologie privée et sera la passerelle par défaut pour tous les PC (si le DHCP n'est pas activé).
2. **Une typologie d'IP statique avec Point-(multi)Point (publique)**. Dans ce cas il faudra configurer la section WAN-ISP comme suit : NAT= habilité et IP address = adresse IP publique et statique assignées (ceux du point-point), Subnet mask et Default Gateway (qui sera une adresse IP publique) seront fournies par le FAI. Le LAN IP sera toujours une IP statique publique et fera partie de la typologie assignée avec le subnet mask. Les autres IP de cette typologie (et la subnet mask) devront être sur les PC avec la passerelle par défaut qui sera le LAN-IP (et les DNS).
3. **Une typologie d'IP statique avec Point-(multi)Point (non publique)**. Dans ce cas il faudra configurer la section WAN-ISP comme suit : NAT= désactivé et IP address = adresse IP publique et statique assignées (ceux du point-point), Subnet mask et Default Gateway (qui sera une adresse IP publique) seront fournies par le FAI. Le LAN IP fera au contraire parti de la typologie assignée avec le subnet mask. Les autres IP de cette typologie (et la subnet mask) devront être sur le PC avec la passerelle par défaut qui sera le LAN-IP (et les DNS).

Paramètres à configurer:

L'illustration ci-dessous apparaîtra (à contrôler attentivement):



- **Description:** le type de connexion.
- **VPI/VCI:** demander les paramètres de configuration à votre opérateur (FAI).
  - **VPI = 8, 8, 2**

- **VCI = 67, 35, 32**

- **NAT:** choisir **Valide(Enable)** (selon le contract).
- **Méthode d'encapsulation(Encapsulation) = LLC Routed**. Demander les paramètres de configuration à votre opérateur (FAI).

Cocher **Utiliser l'adresse IP suivante** :

- **Adresse IP(Static IP Address)=** introduisez l'adresse IP.
- **Masque de sous réseau(Subnet Mask)=** introduisez le masque de sous-réseau.
- **Passerelle(Gateway)=** remplissez les champs suivants avec les caractéristiques de votre abonnement ADSL (l'adresse IP du Default Gateway).
- **RIP:** Invalide

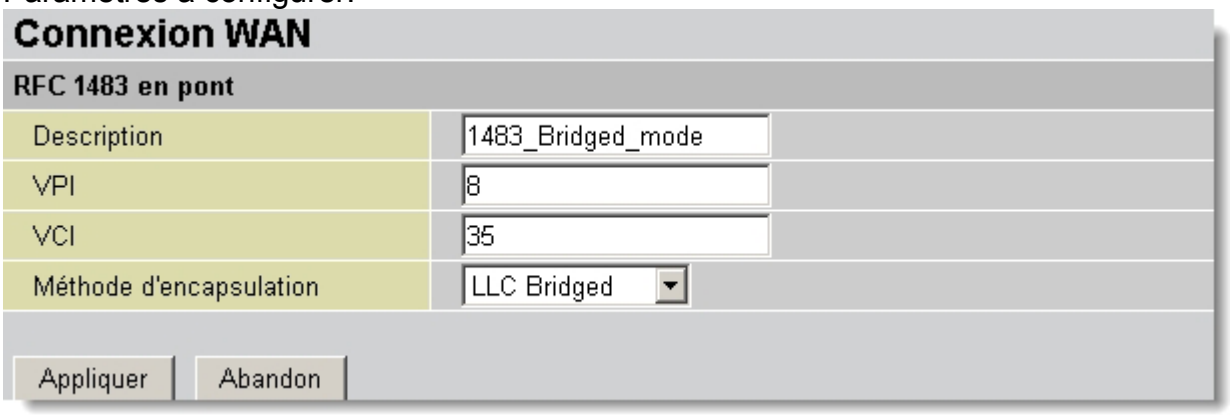
En cliquant sur **Appliquer (Apply)**, le Wireless Routeur ADSL2+ fera un reboot automatique [**La LED ADSL doit être Allumée fixe** lorsque la session est connectée], votre PC sera alors prêt pour la navigation.Cliquez sur **Sauvegarde en mémoire** (**Save Config to Flash**) pour terminer.

Rappel : il faut mettre les PC avec les DNS. Dans le cas d'une adresse IP unique, dans la section NAT choisir **Enable** par défaut. Si vous avez des adresses publiques, le NAT doit être désactivé.

RFC1483 en Pont [BRIDGE (PPPoE)]

Dans cette configuration, le Routeur fonctionne comme Bridge, il gère donc l'adresse IP publique fournie par le fournisseur d'accès internet **(l'abonnement doit être du type PPPoE)** au PC du Client. Certaines fonctions (Virtual Server) sont désactivées. Cette modalité peut s'avérer nécessaire pour le fonctionnement de certains logiciels internet.

Paramètres à configurer:

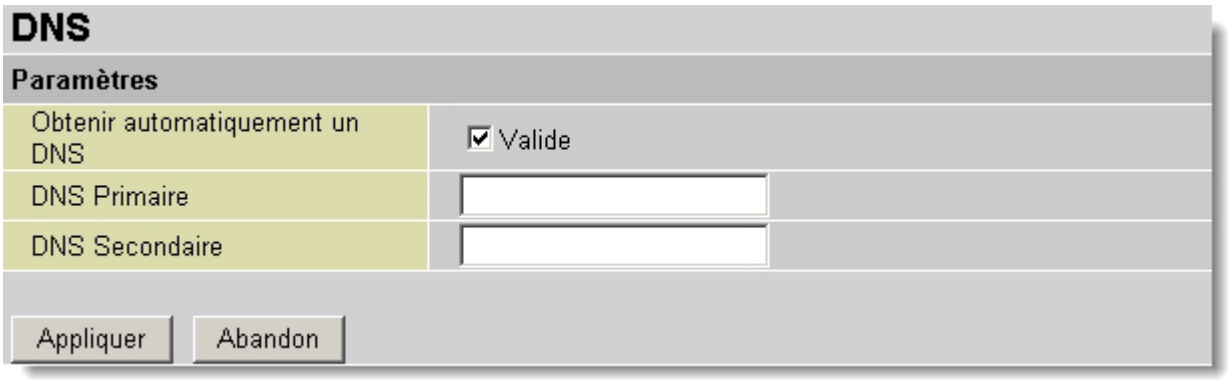


- **Description:** le type de connexion.
- **VPI/VCI:** demander les paramètres de configuration à votre opérateur (FAI).
  - **VPI = 8, 8, 2**
  - **VCI** = **67, 35, 32**
  - **Méthode d'encapsulation (Encapsulation) =** Choisir **LLC Bridged**.

En cliquant sur **Appliquer(Apply)**, le Wireless Routeur ADSL2+ fera un reboot automatique [La LED **ADSL doit être Allumée fixe** lorsque la session est connectée], votre PC sera alors prêt pour la navigation. Cliquez sur **Sauvegarde en mémoire (Save Config to Flash)** pour terminer.

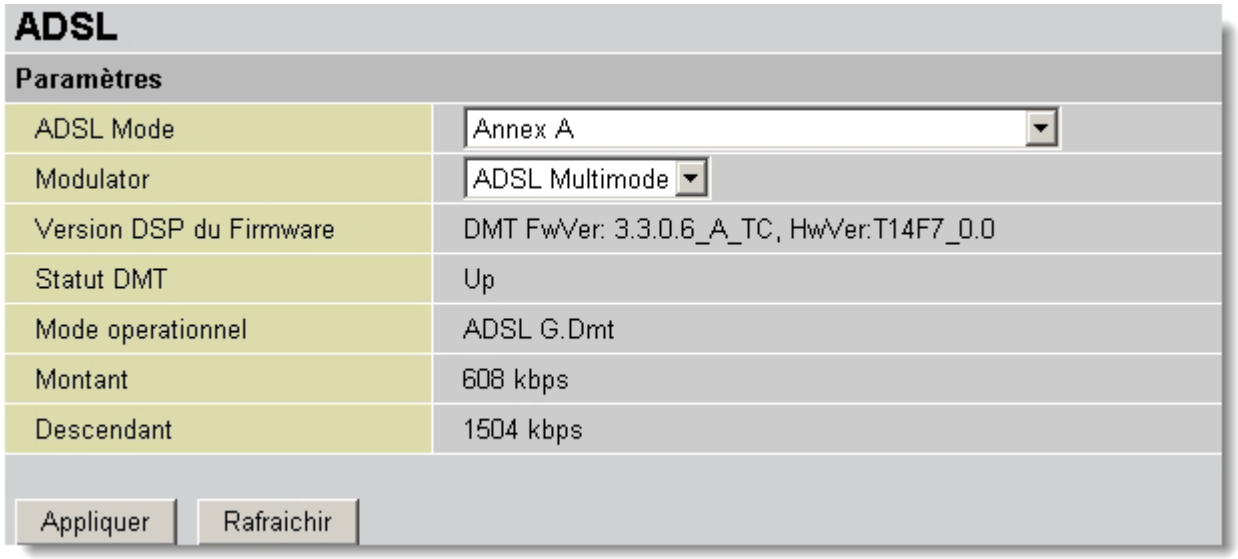
A ce point il ne reste plus qu'à installer sur le PC, le client PPPoE, par exemple le RASPPPOE ou d'utiliser celui intégré dans le Système Opérationnel (dans le cas de Windows XP ou MacOS X). Pour de plus amples renseignements sur l'utilisation du Client PPPoE intégré dans XP, consulter le chapitre 4.

3.6.3.2.2 DNS



Un Domain Name System (DNS) est composé d'un tableau de correspondance entre noms de site et adresses IP publiques. Sur Internet un site possède un seul nom comme www.yahoo.com et une adresse IP. L'adresse IP est difficile à mémoriser (mais c'est toujours la méthode la plus efficace). Cette tache est gérée par le DNs qui grâce au tableau, fournit au PC demandant l'adresse IP correspondant au nom du site (et au cas ou il n'y arrive pas, il le fera à travers d'autres serveurs DNS dont il connaît l'IP). Les adresses IP des DNS seront fournies par le FAI au moment du LogOn (si on utilise le PPPoA/PPPoE ou RFC1483 Bridge). Si le protocole est RFC 1483 Routed ou IpoA (RFC 1577) il est nécessaire d'introduire manuellement les adresse IP des DNS du FAI.

3.6.3.2.3 ADSL



ADSL Mode: 3 choix sont disponibles "**Annex A**","**Annex L**" et "**Annex M"**.
Modulator: 4 choix "**AUTO**","**ADSL**","**ADSL2**" et "**ADSL2+**". En choisissant **Automatique(Auto),** il détecte automatiquement le code de ligne ADSL.
Version DSP du Firmware (DSP Firmware Version): Version du Firmware du code ligne ADSL.
Connected (Connecté): Indique le statut actuel de la synchronisation de ligne ADSL.
Mode Opérationnel (Operation Mode): Indique lorsque le Router et la ligne ADSL sont synchronisés.
Annexe Type: ADSL Annexe A, fonctionne avec une ligne de téléphone standard. Annexe B, fonctionne avec une ligne ISDN.
Débit Montant(Upstream): Indique le débit montant de votre ligne ADSL.
Débit descendant (Downstream): Indique le débit descendant de votre ligne ADSL.

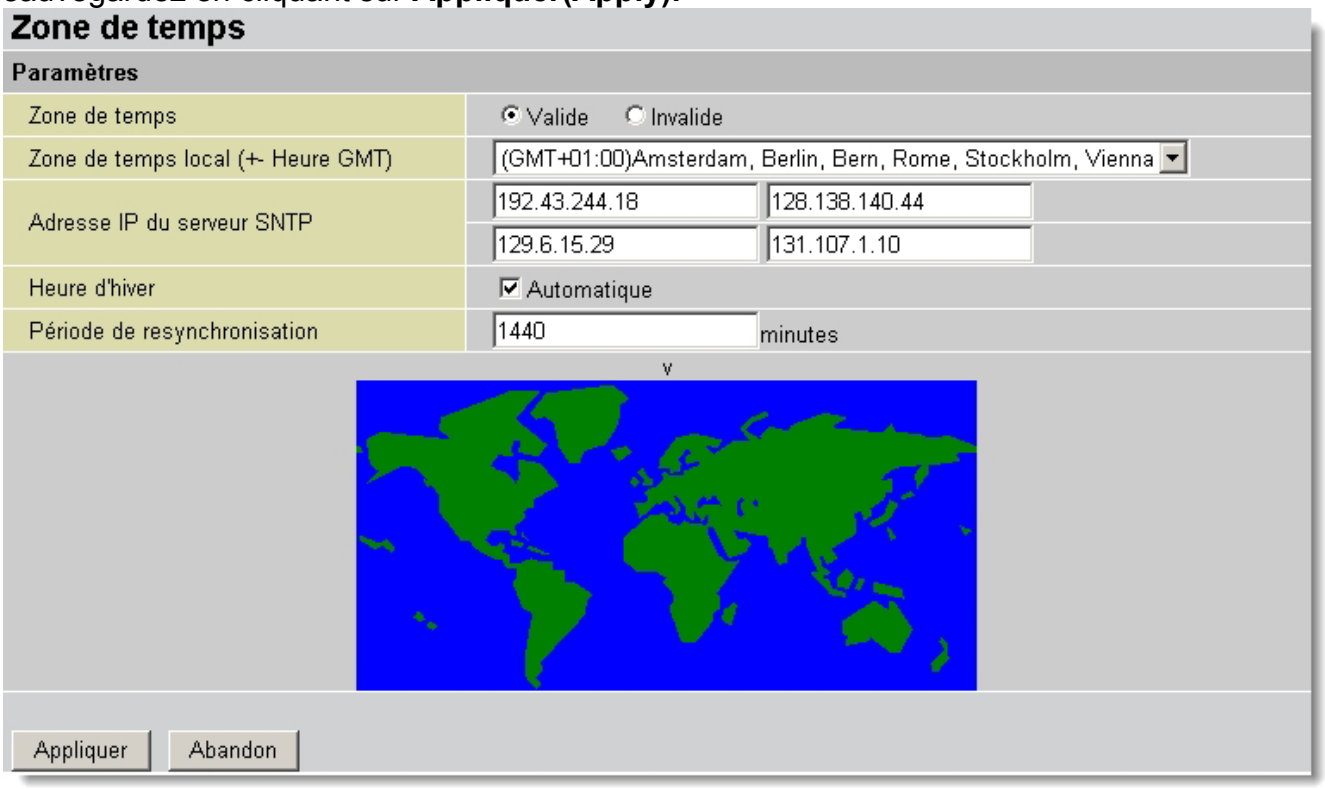
3.6.3.3 SYSTEME (System)

En cliquant sur le menu **Configuration,** les menus suivants apparâitront:

- **Zone de Temps(Time Zone)**
- **Accès distant (Remote Access)**
- **Mise à jour du firmware (Firmware Upgrade)**
- **Sauvegarde/Restauration (Backup/Restore)**
- **Redémarrage (Restart)**
- **Gestion des utilisateurs (User Management)**

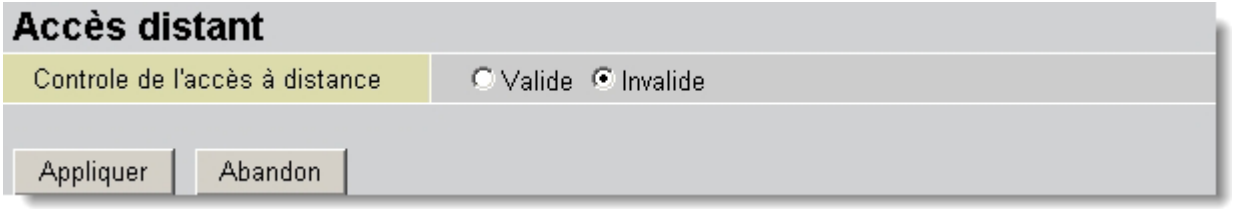
3.6.3.3.1 Zone de temps (Time Zone)

Le routeur n'a pas d'horloge en temps réel, à la place il emploie le Simple Network Time Protocol (SNTP) pour obtenir l'heure du serveur de SNTP. Choisissez votre fuseau horaire et sauvegardez en cliquant sur **Appliquer(Apply).**



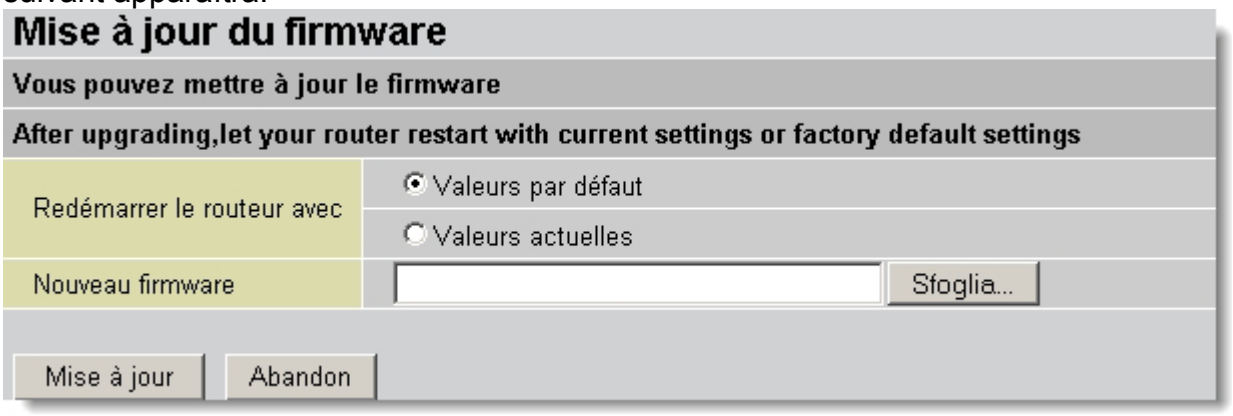
3.6.3.3.2 Accès Distant (Remote Access)

Pour autoriser l'administration à distance de votre routeur.



3.6.3.3.3 Mise à jour (Firmware Upgrade)

Pour améliorer le firmware (microprogramme) du routeur, vous devez préalablement le télécharger ou copier sur votre réseau local, de préférence sur la machine servant à configurer le routeur.
Ensuite dans le menu **Configuration** puis **Système** choix **Mise à jour du firmware**. L'ecran suivant apparaîtra.


Mise à jour du firmware
Vous pouvez mettre à jour le firmware
After upgrading,let your router restart with current settings or factory default settings
Redémarrer le routeur avec
Valeurs par défaut
Valeurs actuelles
Nouveau firmware
Sfoglia...
Mise à jour
Abandon

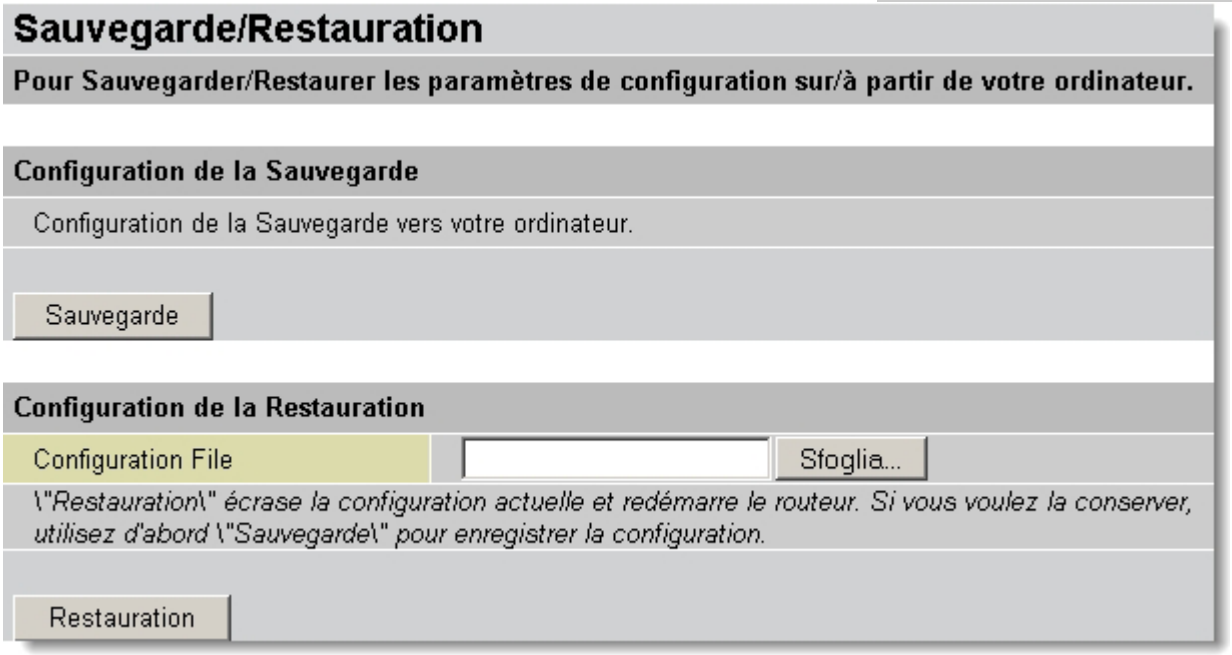
Cliquez sur **Sfoglia** puis indiquez le chemin d'accès au firmware. Cliquez sur le bouton **Mise à Jour(Upgrade)** pour commencer la mise à jour du firmware.

ATTENTION : l'alimentation électrique du Router ADSL, pendant la phase entière d'upgrade, ne doit pas être coupée. Sous peine de rendre l'appareil inutilisable.
Détacher le câble RJ11 du router. Effectuer l'upgrade en utilisant une connexion filaire et surtout pas sans fil.
Cela pourrait endommager le routeur et rendre caduque la garantie.

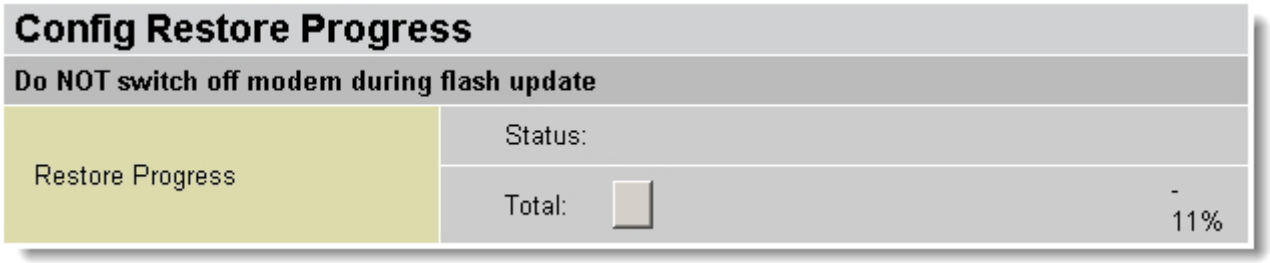
Le Routeur effectuera le reboot en chargeant le nouveau firmware avec la configuration initiale (si vous avez **choisi Valeurs par défaut**).

3.6.3.3.4 Sauvegarde/Restauration (Backup / Restore)

Le Wireless Routeur ADSL2+ permet d'effectuer un backup sur (ou à partir de) le disque dur de votre PC. Grâce à cette fonction, il sera possible de sauvegarder des configurations complexes et rendre à nouveau opérationnel le Routeur en peu de temps.

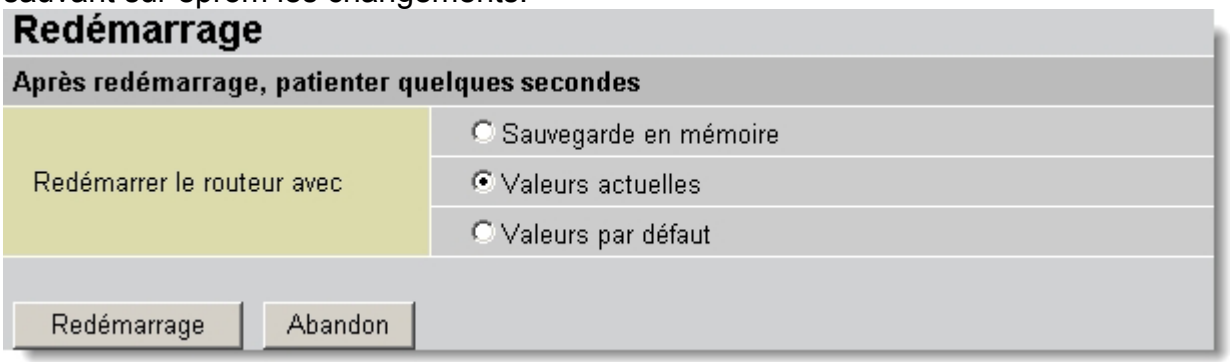

Sauvegarde/Restauration
Pour Sauvegarder/Restaurer les paramètres de configuration sur/à partir de votre ordinateur.
Configuration de la Sauvegarde
Configuration de la Sauvegarde vers votre ordinateur.
Sauvegarde
Configuration de la Restauration
Configuration File
Sfoglia...
\"Restauration\" écrase la configuration actuelle et redémarre le routeur. Si vous voulez la conserver, utilisez d'abord \"Sauvegarde\" pour enregistrer la configuration.
Restauration

Pour effectuer le backup cliquez sur le bouton **Sauvegarde(Backup).** Il vous reste seulement à sélectionner le chemin ou vous voulez sauvegarder les données de configuration (le fichier crée aura une extension .CFG)
Pour effectuer la récupération cliquez sur le bouton **Sfoglia** en indiquant le chemin qui contient le fichier de configuration puis cliquez sur **Restauration(Restore)**.
Pendant le Restore l'image suivante apparaîtra.



3.6.3.3.5 Redémarrage (Restart)

Si par nécessité, on doit reconfigurer le routeur ADSL avec la configuration par défaut (en perdant tous les réglages personnalisés), il suffira d'accéder via le menu **Configuration-Système** à la commande **Redémarrage(Restart Routeur)** et cocher **Valeurs par défaut(Factory default settings)**. Cliquez ensuite sur le bouton **Redémarrage(Restart Routeur)** (pour de plus amples informations, veuillez consulter la section 3.4)
Au contraire, en cliquant seulement sur le bouton **Redémarrage(Restart)** le routeur effectuera un simple redémarrage (reboot). Après chaque changement, pensez à cliquer le bouton **Sauvegarde en mémoire** (**Save config to Flash)** pour les rendre permanent en sauvant sur eprom les changements.

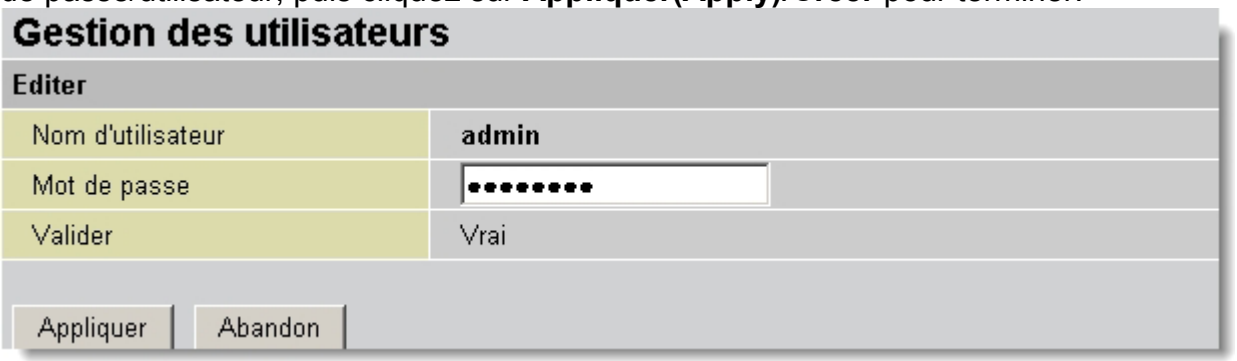


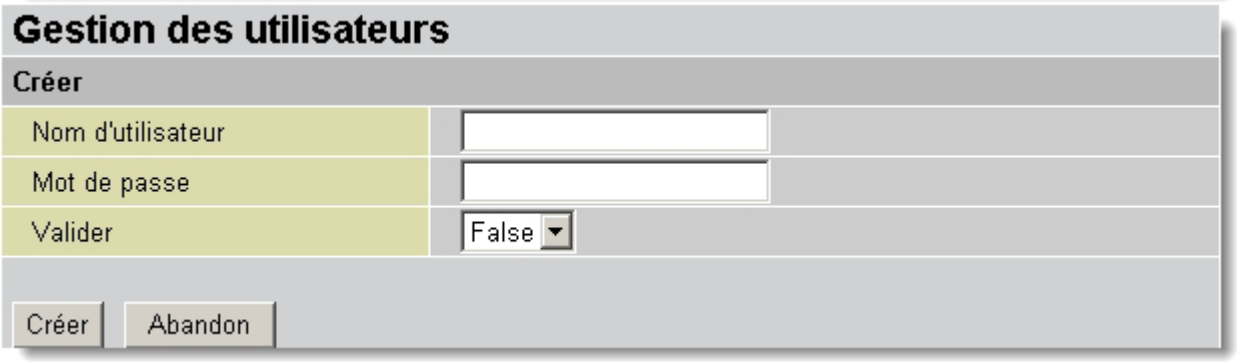
3.6.3.3.6 Gestion des utilisateurs (User Management)

Vous pouvez changer le mot de passe d'accès.

Allez dans le menu **Configuration-Système** puis dans la fonction **Gestion des utilisateurs** (**User Management),** le choix suivant apparaîtra:

Il faut cliquer sur **Editer** (pour changer le mot de passe) ou sur **Créer**, mettre le nouveau mot de passe/utilisateur, puis cliquez sur **Appliquer(Apply)/Crèer** pour terminer.





En cas d'oubli de votre Mot de passe d'accès, vous pouvez ramener le Routeur aux conditions initiales en exécutant la procédure suivante:

Lorsque le routeur est allumé, pressez pour effectuer le reset jusqu'à la fin du clignotement des LEDs, puis rédemarrez le routeur avec la touche Power On/Off.

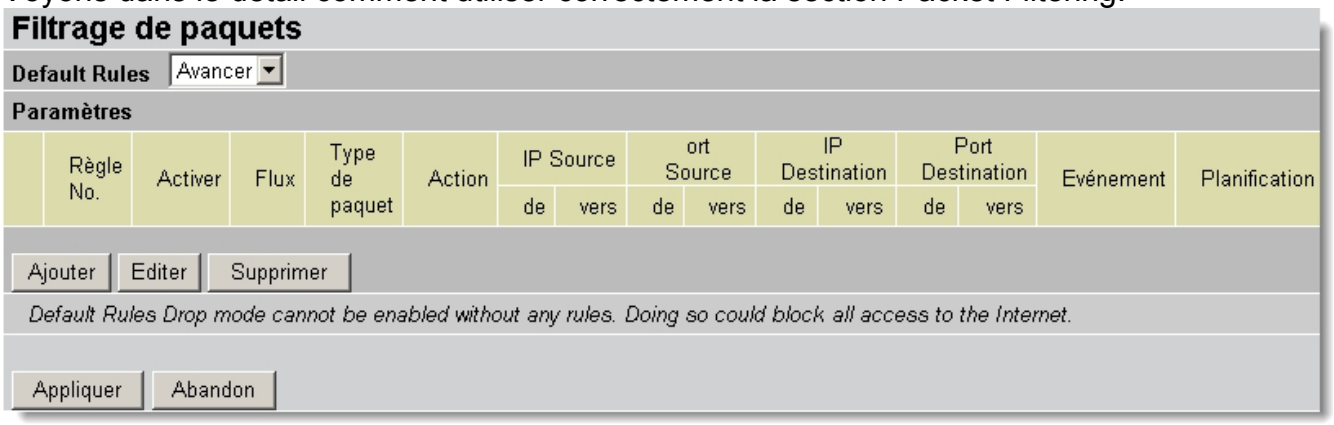
3.6.3.4 Pare Feu (Firewall)

Ce menu permet de configurer un certain nombre de paramètres de sécurité du routeur. Les sous menus sont les suivants :

- **Filtrage de paquets (Packet Filtering)**
- **Filtrage par adresse MAC (MAC Filtering)**
- **Détection d'intrusion (Intrusion Detection)**
- **Blocage de requête WAN (Block WAN Request)**
- **Filtrage d'URL (URL Filter)**

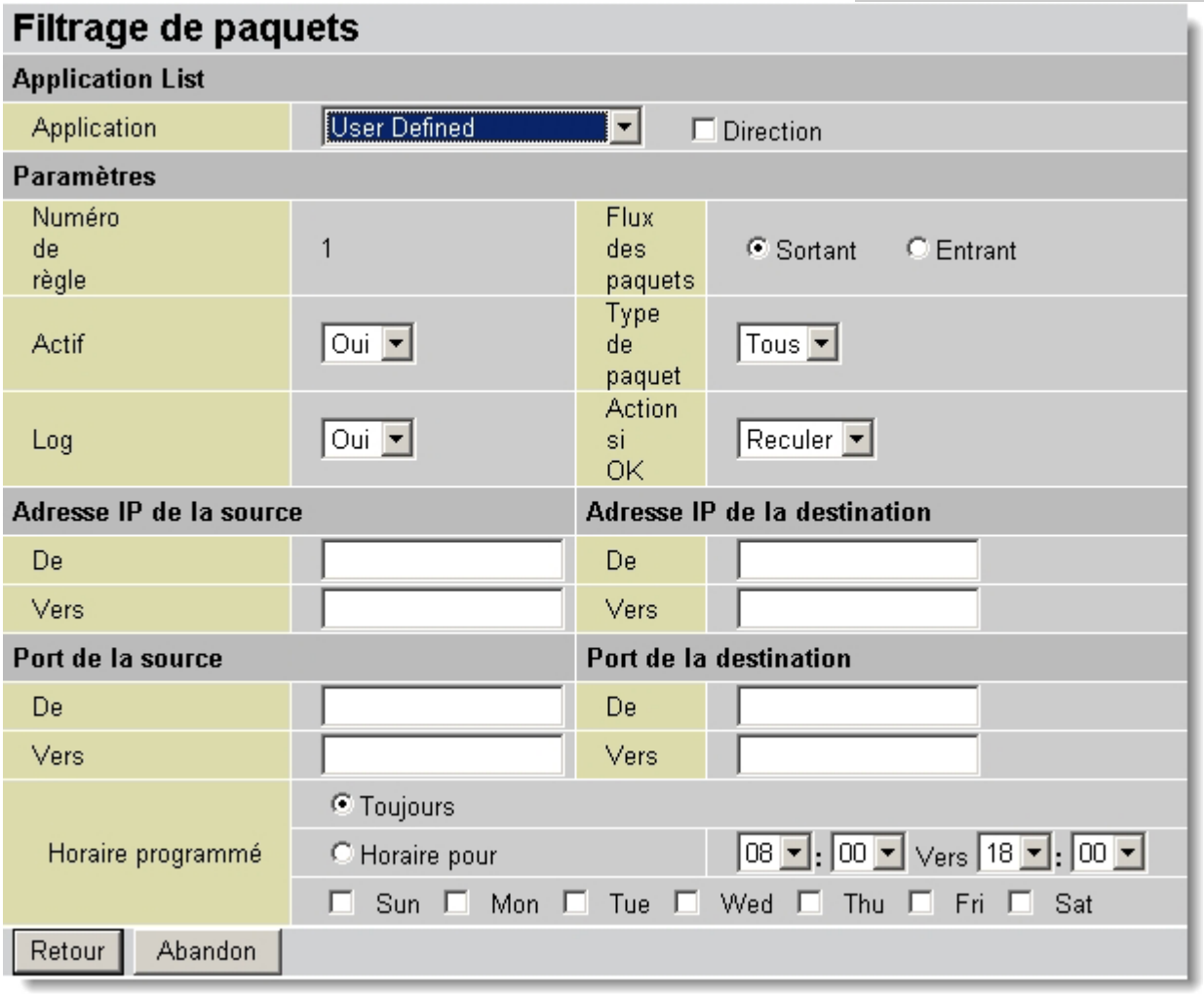
3.6.3.4.1 Filtrage de paquets (Packet Filtering)

Cette fonction de filtrage de paquets IP permet d'établir une série de règles que le Wireless Router ADSL2+ appliquera aux paquets qui le traversent (il vérifira l'application de ces règles, paquet par paquet). Il est important de savoir que le filtrage seul, n'élimine pas tous les problèmes liés aux applications. Vous pouvez utiliser jusqu'à 10 règles.
Voyons dans le détail comment utiliser correctement la section Packet Filtering.



Vous pouvez utiliser toute une série de règles pour avoir un contrôle proportionné à vos attentes. La relation logique entre les règles est de type **OU**, le Firewall teste le paquet qui le traverse, à partir de la règle numéro 1 puis lorsque la règle est satisfaite, l'action spécifique est exécutée (le paquet n'est pas examiné par les règles suivantes).
Le bouton **Editer(Edit)** permet, après avoir choisi le numéro de la règle, de la modifier.
Le bouton **Supprimer(Delete)** permet, après avoir choisi le numéro de la règle, de l'éliminer.
Le bouton **Ajouter(Add)** permet d'accéder au tableau suivant, pour construire une nouvelle règle.

Avant de choisir **Reculer** il faut mettre avant une série de règles pour faire passer les paquets.



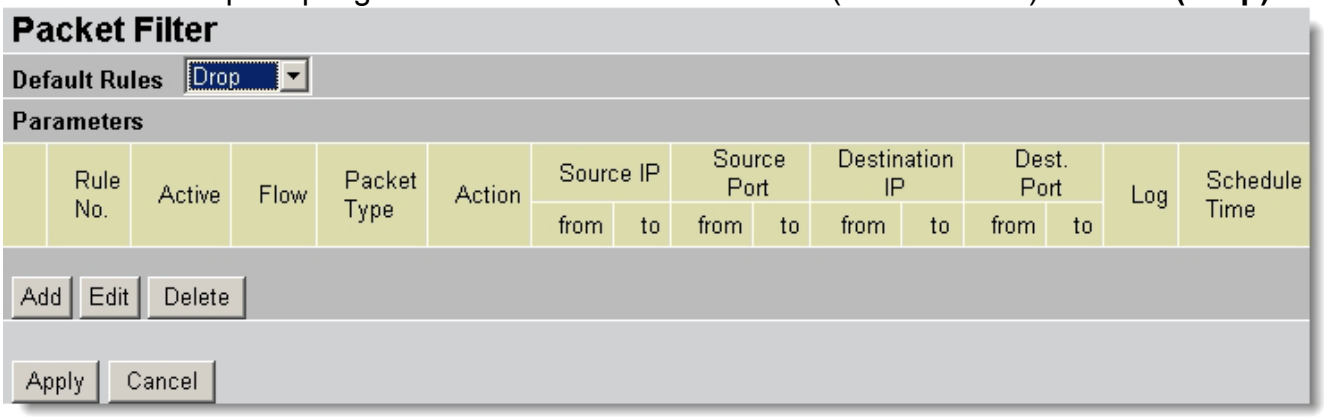
Pour la signification des différents choix (voyez l'appendice B, parcours des paquets IP):

- **Application** :Vous pouvez choisir le service. Seulement en choisissant un service dans la listedifferent de User Defined la voix **direction** (pour les paquets de retour) est active.
- **Flux de paquets [Sortant/Entrant] (⊙ Outgoing / ⊙ Incoming):** Il détermine sur quel type de paquets la règle doit être appliquée, paquets sortants ou entrants.
- **Actif(Active):** Choisir "Yes" pour valider ou "Non" pour désactiver la règle.
- **Log:** En sélectionnant l'option **YES,** on peut relever des traces détaillées sur ce que fait le firewall. Visualisation dans la section **Status–Security Log**.
- **Type de Paquet(Packet Type):** Spécifier le type de paquets sur lesquels la règle sera appliquée (TCP, UDP, ICMP ou Tous)
- **Action si OK(Action When Matched):** Quand un paquet satisfait à la règle, il est nécessaire de définir l'action qui doit être appliquée: (drop) pour éliminer le paquet ou (forward) pour le faire passer.
- **Adresse IP de la source De (Source IP Address from):** Introduire l'adresse IP (initiale) et finale, source des paquets.
- **Adresse IP de la source Vers (Source IP Address to):** Introduire l'adresse IP (finale), source des paquets.
- **Adresse IP de la Destination De (Destination IP Address from):** Introduire l'adresse IP (initiale), destinataire des paquets.

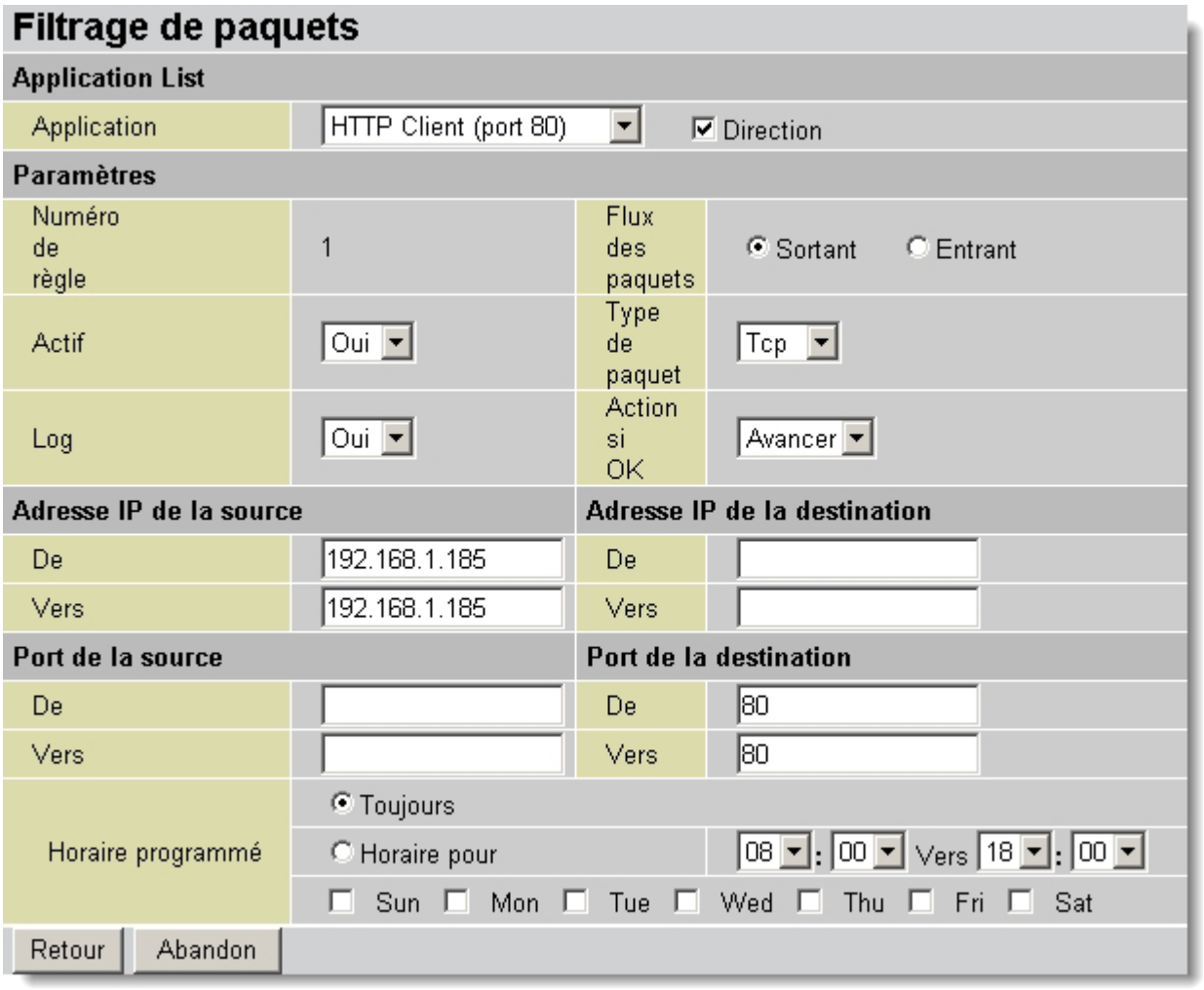
- **Adresse IP de la Destination Vers (Destination IP Address to):** Introduire l'adresse IP (finale), destinataire des paquets.
- **Port de la Source De/Vers (Source Port from/to):** Numéro de port source (initiale/finale) à contrôler, pour TCP ou UDP.
- **Port de la Destination De/Vers (Destination Port from/to):** Numéro de port de destination (initiale/finale) à contrôler pour TCP ou UDP.
- **Schedule Time :** Choisir **Toujours**(**Always)** pour activer toujours les regles ou choisir la période ou les règles seront appliquées (en cochant le jour et l'heure).

Il faut prêter une attention particulière aux ports entrants ou sortants dans la typologie de paquets. Si on désire filtrer l'http, il faut utiliser un filtre pour les paquets entrants ou sortants. Si le filtre est appliqué aux paquets sortants, il faudra sélectionner comme port de destination (Destination) le port 80. Si le filtre est appliqué par contre aux paquets entrants le port de provenance (Source) doit être aussi le port 80. Vous pouvez aussi choisir dans application la voix http (qui la voix direction activée) pour obtenir la meme chose avec une seule regle. Pour toutes autres documentations, utiliser un guide sur l'usage des ports en TCP/IP.

Maintenant, voyons un cas pratique pour exemple:
Exemple : Construisons une série de règles en utilisant une approche conservative. Quand on active le Firewall, seuls les ports explicitement accordés sont permis, le reste est coupé, nous ferons donc transiter lesdonnées par une série de règles. En conclusion, chaque service qui n'est pas explicitement permis est coupé.
Il faut choisir la politique générale avant tout. Dans ce cas (default Rules)=**Reculer(Drop).**

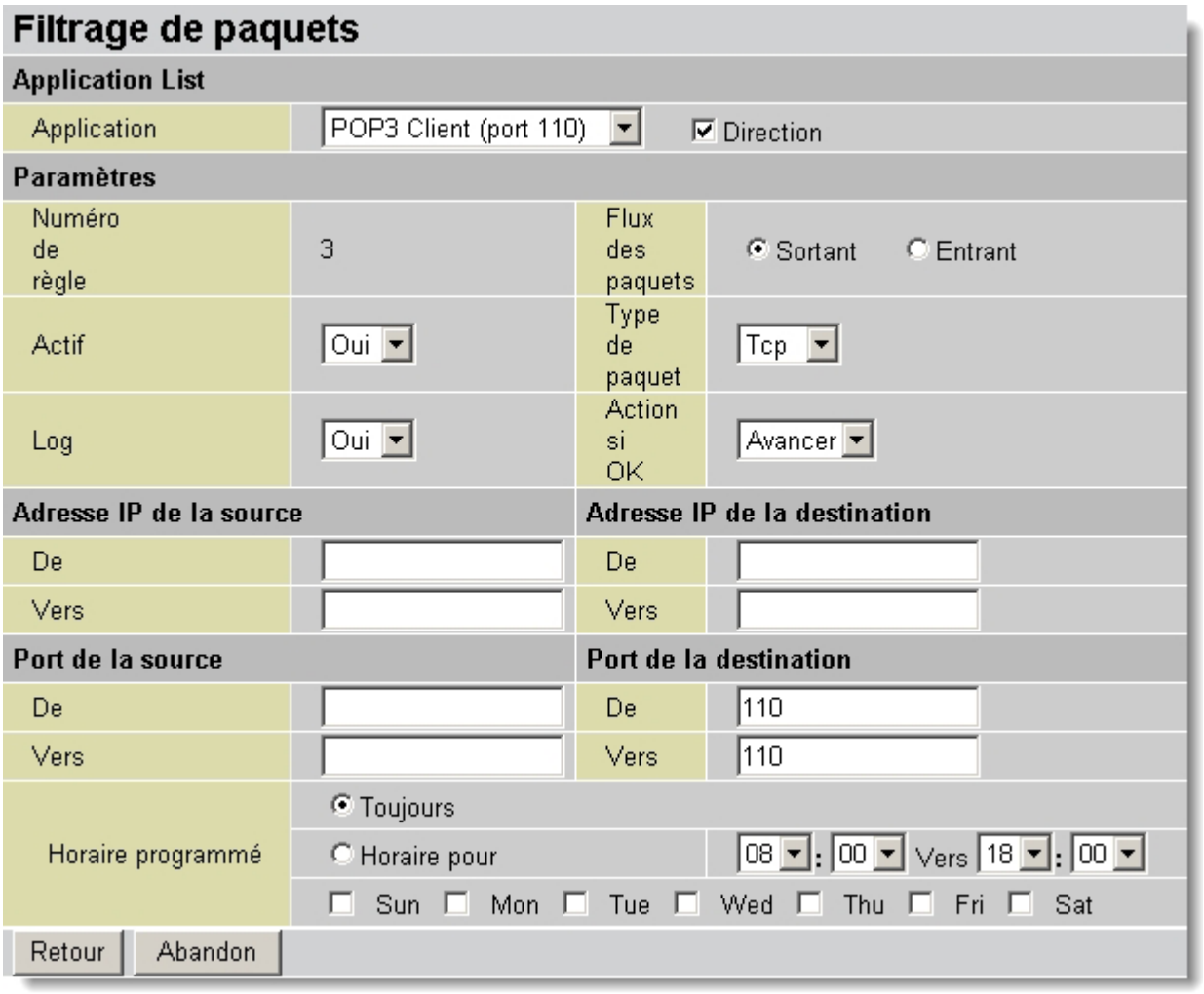


Filtre HTTP:

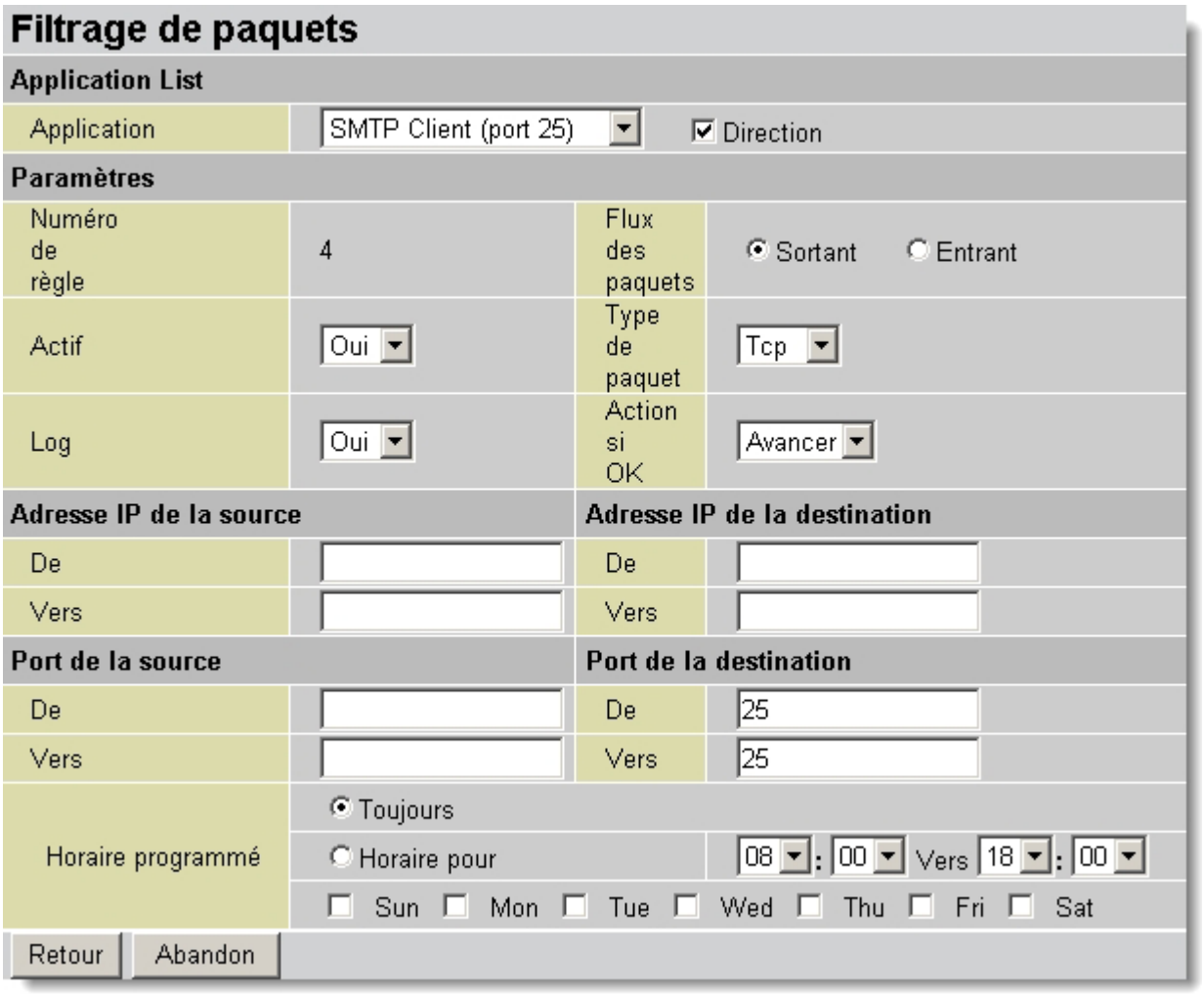


Avec ce règle, tout le trafic sortant et entrant, provenant de n'importe qu'elle adresse IP et adressé à la porte TCP n°80 (nous sommes en train de parler de trafic vers un server WEB), est autorisé par le firewall.

Filtre POP3:

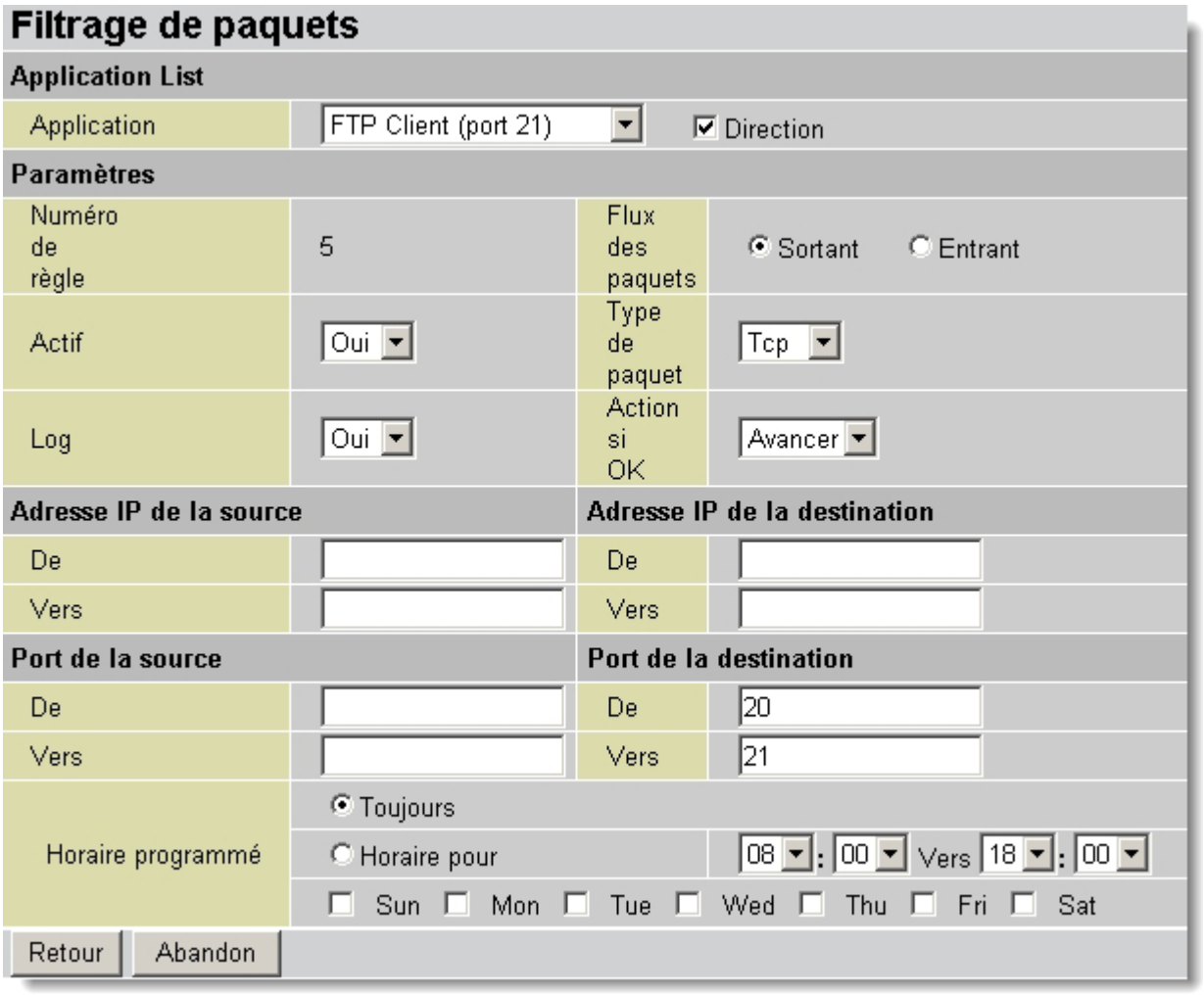

Filtrage de paquets
Application List
Application
POP3 Client (port 110)
Direction
Paramètres
Numéro de règle
3
Flux des paquets
Sortant
Entrant
Actif
Oui
Type de paquet
Tcp
Log
Oui
Action si OK
Avancer
Adresse IP de la source
Adresse IP de la destination
De
Vers
De
Vers
Port de la source
Port de la destination
De
Vers
De
110
Vers
110
Horaire programmé
Toujours
Horaire pour
08 : 00 Vers 18 : 00
Sun Mon Tue Wed Thu Fri Sat
Retour
Abandon

Filtre SMTP:



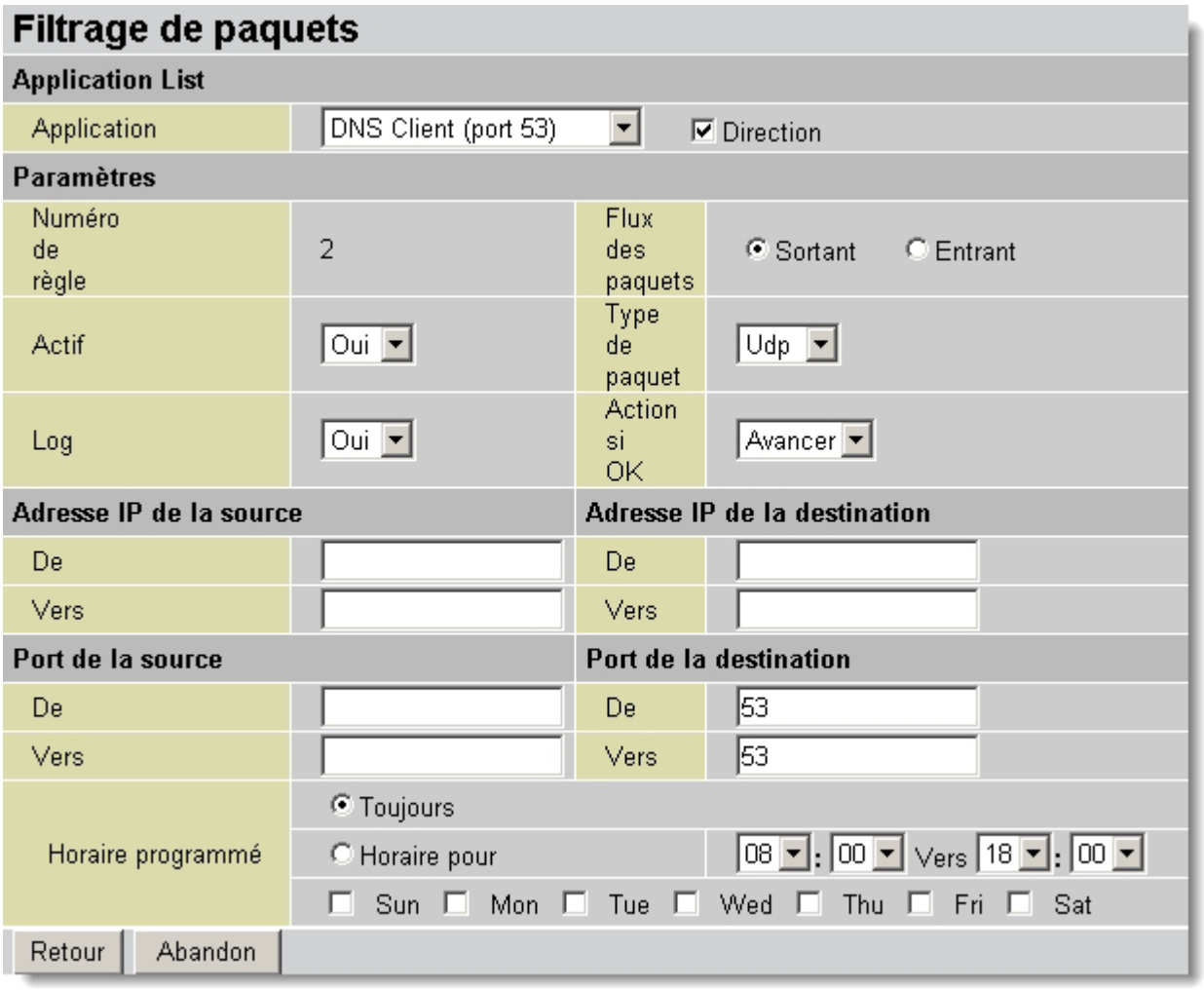
Avec ces 2 règles, tout le trafic sortant, provenant de n'importe qu'elle adresse IP et adressé à n'importe qu'elle adresse IP (en réalité pour les limiter ultérieurement, il faudrait mettre l'adresse IP du POP3 ou du serveur SMTP, selon le cas) et provenant de la porte TCP n°25 ou 110 (on est en train de parler de mail), est autorisé par le firewall.

Filtre FTP :



Avec ce règle, tout le trafic sortant et entrant , provenant de n'importe qu'elle adresse IP et adressé à la porte TCP n°21, (nous sommes en train de parler de trafic vers un server FTP), est autorisé par le firewall.

Filtre DNS :



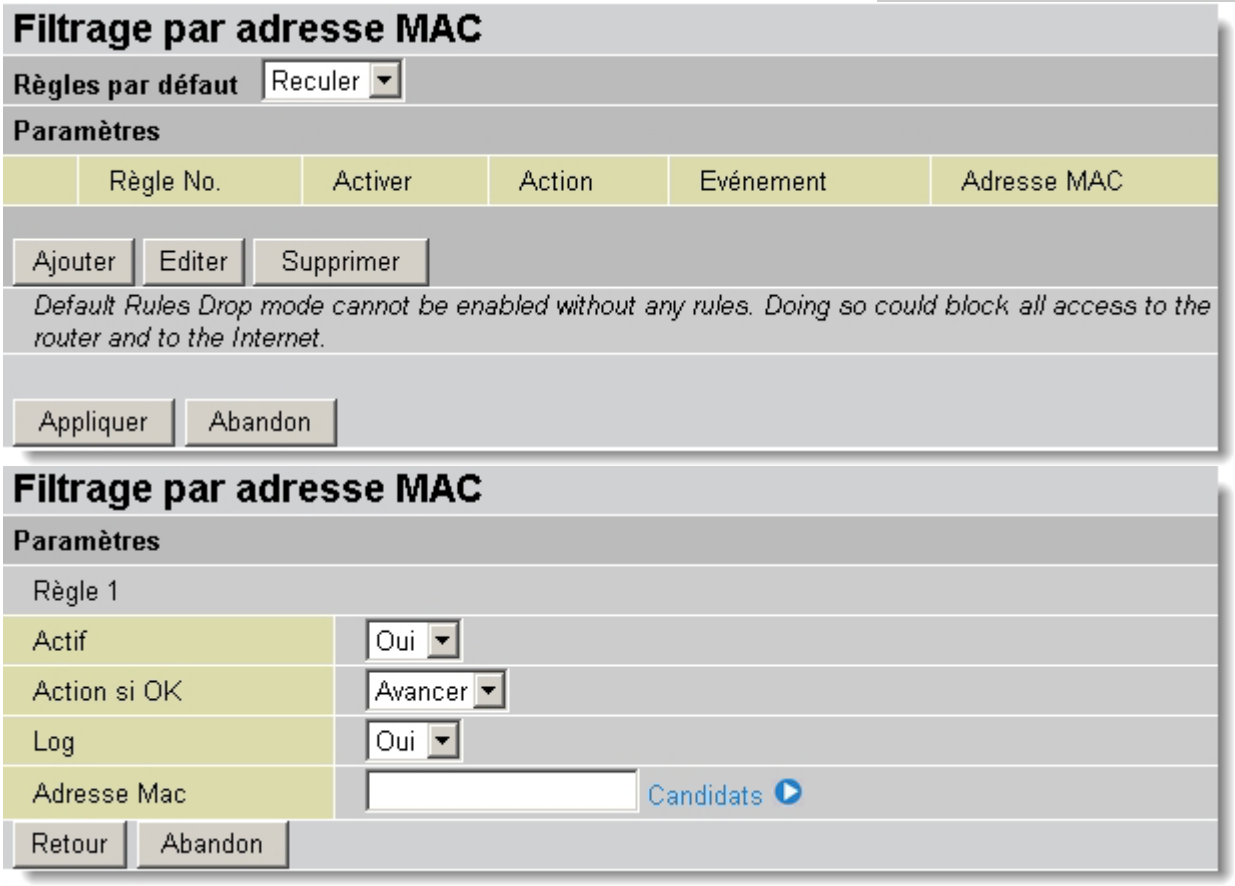
Avec ce règle, tout le trafic sortant et entrant, provenant de n'importe qu'elle adresse IP et adressé à la porte UDP n°53 (nous sommes en train de parler de trafic vers un serveur DNS), est autorisé par le firewall.

3.6.3.4.2 Filtrage par adresse Mac (Mac Filtering)

Permet de filtrer le trafic à partir des adresses MACs des cartes réseaux. Il sera ainsi possible de bloquer ou de permettre l'accès à une liste d'adresses déterminées.

Reculer(Drop)= Seules les adresses MACs de la liste (avec **Action si OK=Avancer**) peuvent accéder au Routeur, les autres sont bloquées.

Avancer(Forward)= Toutes les adresses MACs peuvent accéder au Routeur, seules les adresses MACs de la liste (avec **Action si OK= Reculer**) sont bloquées.

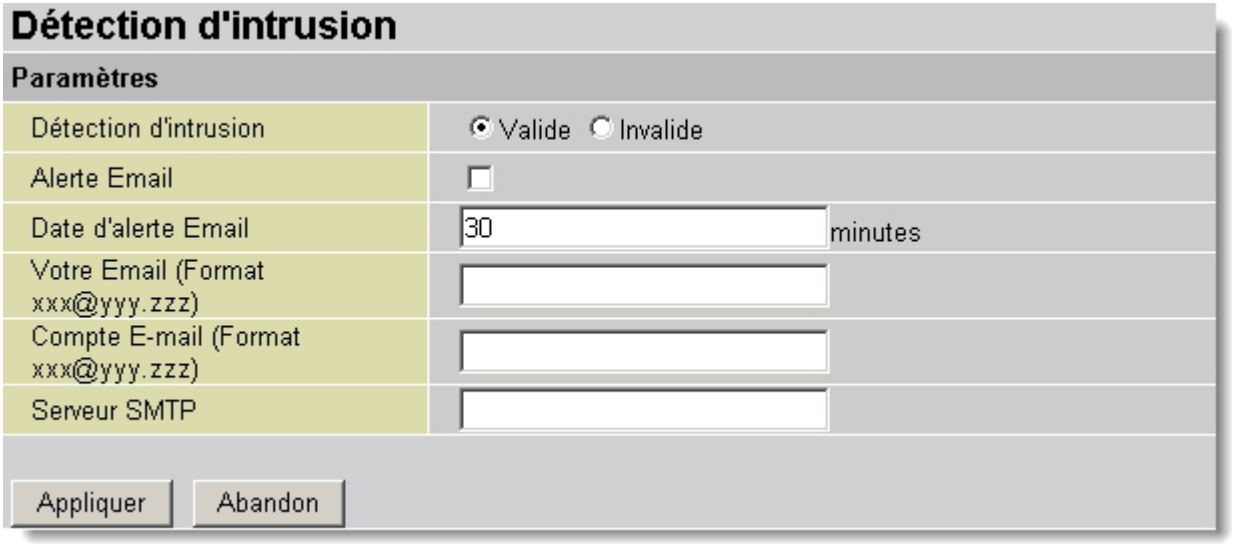


- **Actif(Active):** Selectionnez Oui(**Yes)** pour mettre en route la fonction.
- **Action si OK(Action When Matched):** Selectionnez “Reculer(Drop)” ou “Avancer(Forward)”.
- **Log:** Choisissez “Oui(Yes)”, si vous voulez génerer un rapport d’évenement à chaque fois que la règle est appliquée à un paquet.
- **Adresse MAC(MAC Address):** Entrez l’adresse MAC à gérer.
- **Candidats :** Vous pouvez voir la liste des MACs connectés au routeur entre les quels choisir.

3.6.3.4.3 Detection d'Intrusion (Intrusion Detection)

Pour reconnaître et bloquer automatiquement, les attaques de type Denial of Service (DoS), le routeur détermine si un paquet de données qui arrive peut être envoyé dans le réseau. La liste des attaques DOS reconnue

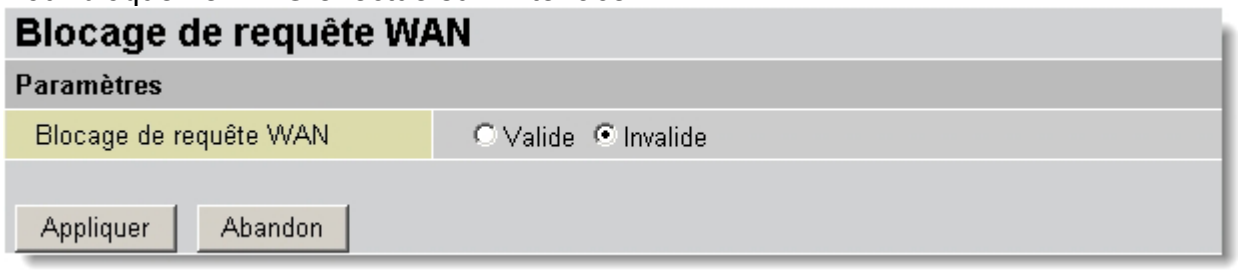
- IP Spoofing
- Ping of Death (Length > 65535)
- Land Attack (Same source / destination IP address)
- IP with zero length
- Sync flooding
- Smurf Attack (ICMP Echo with x.x.x.0 or x.x.x.255)
- Snork Attack
- UDP port loop-back
- TCP NULL scan



Pour faire parvenir un émail d'alerte, après une attaque DOS. Cocher le champ **Alert Mail**, et remplir les renseignements suivants.

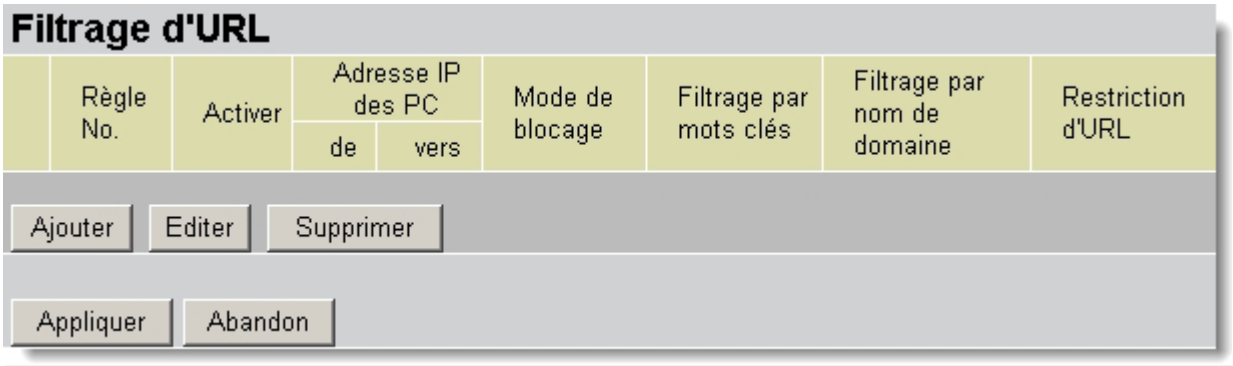
3.6.3.4.4 Blocage d'adresse Wan (Block Wan Request)

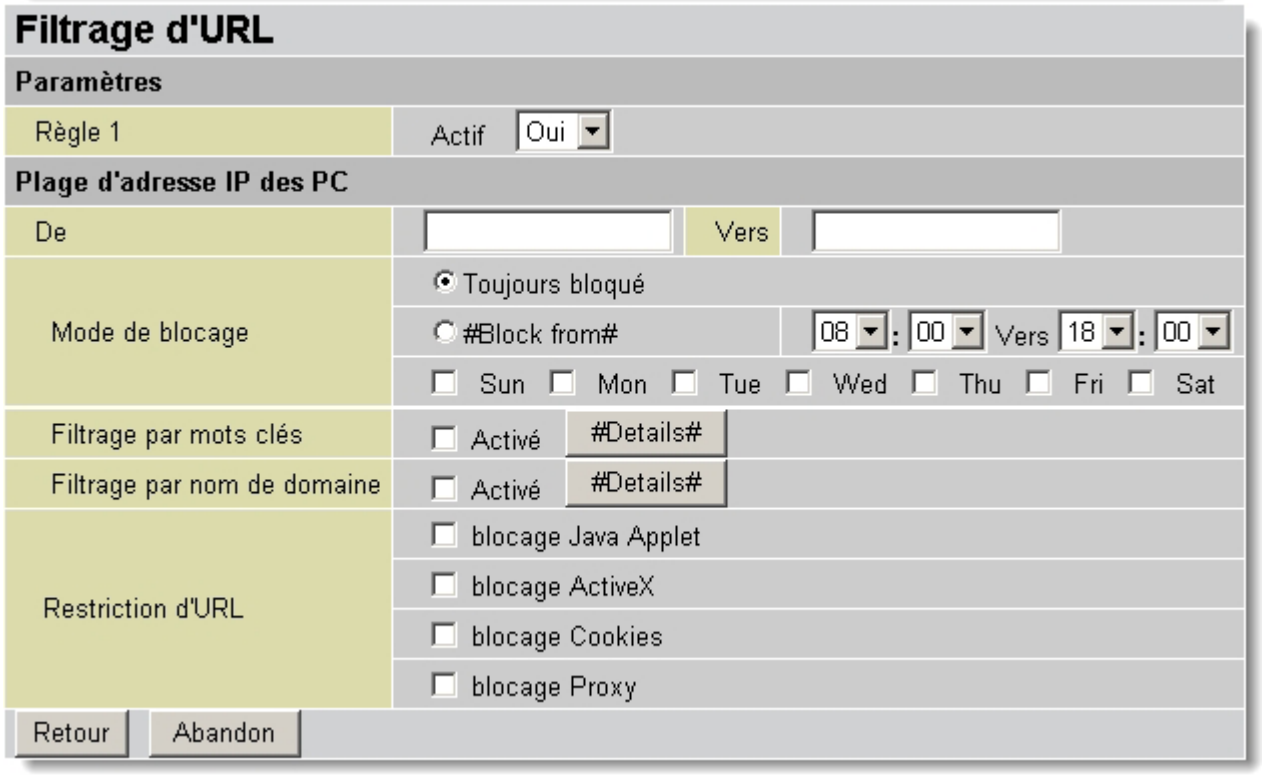
Pour bloquer le PING effectué sur l'interface WAN.



3.6.3.4.5 Filtrage par Url (URL Filtering)

Permet de filtrer le trafic en sortie en le limitant soit par heure et/ou jour soit à une séquence de caractères établis. Permet aussi de filtrer le trafic à partir d'URL. Vous pouvez limiter l'usage du routeur à des horaires déterminés.
Vous pouvez utiliser toute une série de règles pour avoir un contrôle proportionné à vos attentes. La relation logique entre les règles est de type **OU**, le Firewall teste le paquet qui le traverse, à partir de la règle numéro 1 puis lorsque la règle est satisfaite, l'action spécifique est exécutée (le paquet n'est pas examiné par les règles suivantes).
Le bouton **Editer (Edit)** permet, après avoir choisi le numéro de la règle, de la modifier.
Le bouton **Supprimer(Delete)** permet, après avoir choisi le numéro de la règle, de l'éliminer.
Le bouton **Ajouter** (**Add)** permet d'accéder au tableau suivant, pour construire une nouvelle règle.





3.6.3.5 QoS

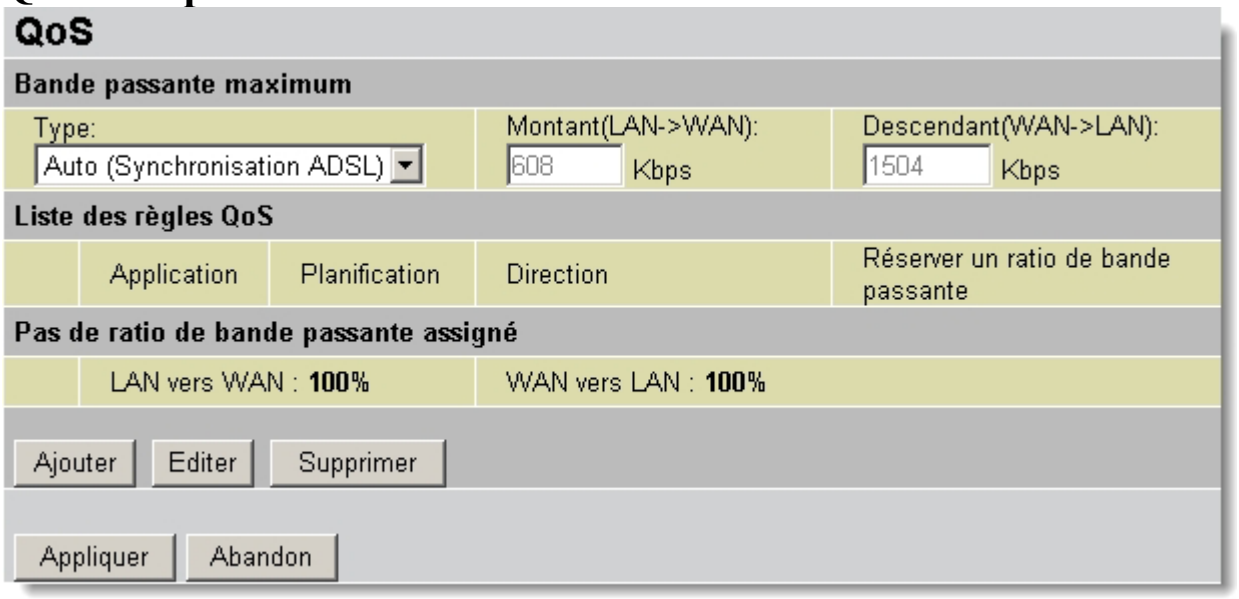
Introduction à la Qualité de Service

Si vous trouvez que votre vitesse de connexion est ralentie parce qu'un autre ordinateur de votre réseau utilise (par exemple) un logiciel de P2P, vous comprendrez pourquoi la Qualité de Service est si importante pour les utilisateurs domestiques ou de bureau.

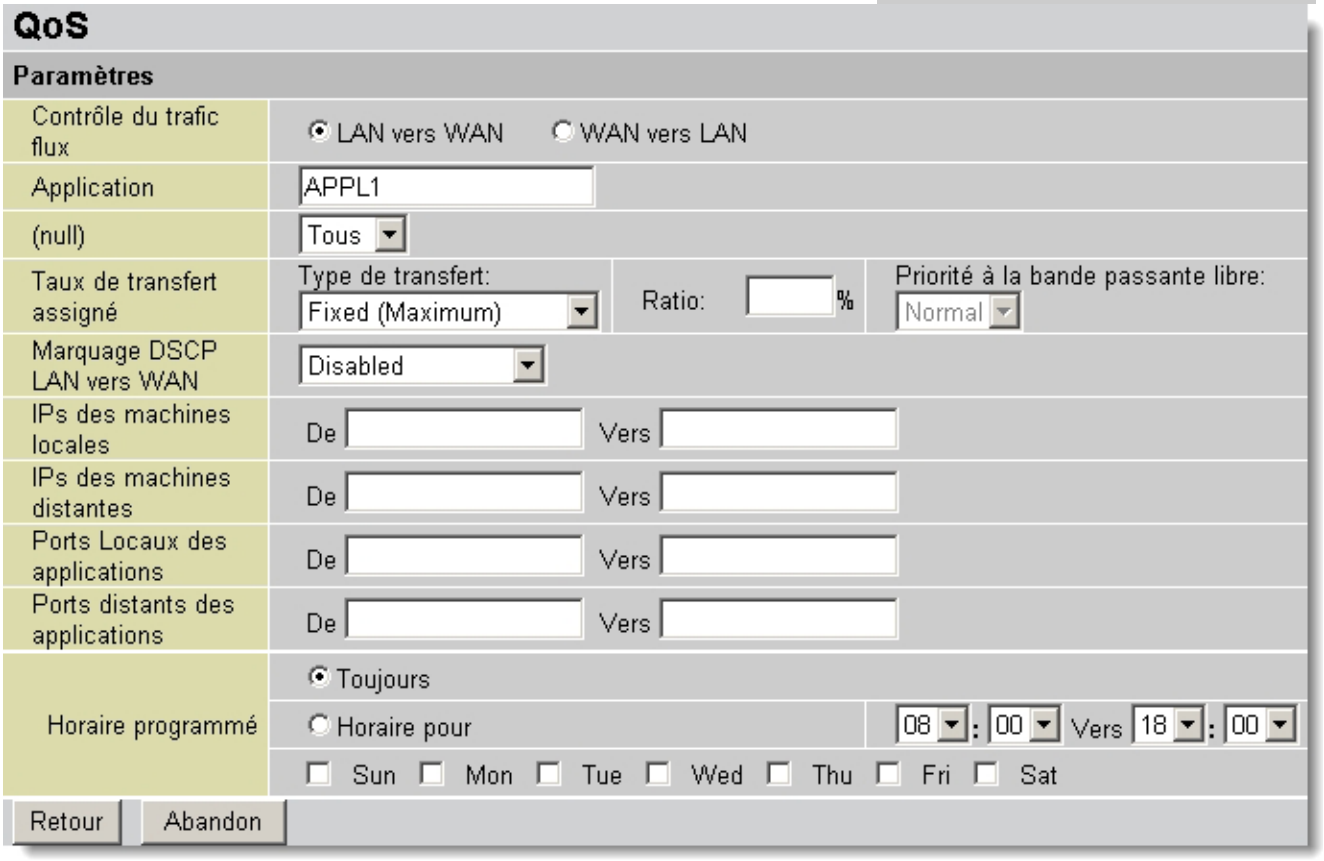
QOS: Pour conserver votre connexion Internet Rapide te Réactive

Configurable par adresse IP (source ou destination), protocole et port, la Qualité de Service (QOS) vous donne le plein contrôle sur la priorité à affecter à chacune des ressources logicielle ou matérielle.

QOS Setup



Après avoir cliqué sur le bouton QOS, vous pouvez **Ajouter/Modifier** ou Supprimer les règles du QOS. Cette page vous indique les différentes règles établies ainsi que la bande passante non attibuée.



Application: Nom identifiant une application.

Time Schedule: Durée d'application de la règle.

Direction: Sens du contrôle entre LAN et WAN.

LAN vers WAN: Vous voulez contrôler le traffic entre votre réseau local et Internet. Exemple type : Serveur FTP sur votre réseau et vous voulez limiter la bande passante qui lui est affectée.

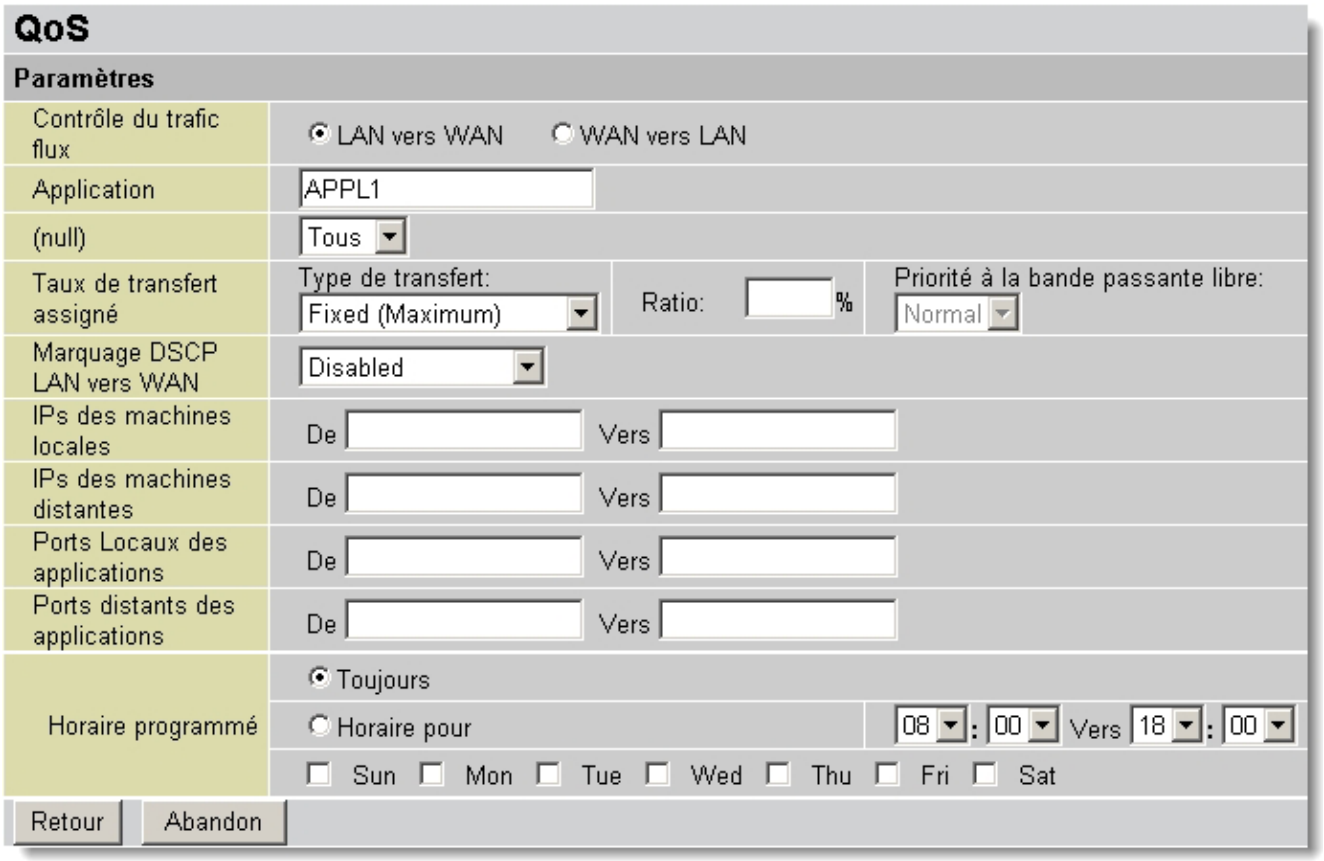
WAN vers LAN: Vous voulez contrôler le traffic entre Internet et votre réseau local.

Taux de Transfert Assigné(Assigned Bandwidth Ratio): Ce champ vous permet de visualiser l'état actuel de vos règles en % de bande passante. Si la connexion à Internet est active, vous pourrez voir les taux de transfert (en kbps). Vous pouvez spécifier un taux de transfert fixe ou minimum garanti avec un degré de priorité d'utilisation de la bande passante non affectée.

Non-Assigned Bandwidth Ratio: Ce champ vous indique les bandes non attribuées (LAN vers WAN et WAN vers LAN).
Cliquez sur le bouton Add pour ajouter une nouvelle règle de QOS.

Avant d'utilisez les boutons **Editer(Edit)/Supprimer(Delete)** pour Modifier ou Supprimer une règle, sélectionnez la avec sa case à cocher.
Après avoir configuré la règle, cliquez sur le bouton Apply pour l'appliquer. Si vous voulez la rendre permanente en l'enregistrant dans la mémoire flash, cliquez sur **Save Config To Flash** dans la partie gauche de la fenêtre.

Lorsque vous cliquez sur **Ajouter(Add)** ou **Editer(Edit),** la fenêtre suivante apparaît.



Contrôle du trafic flux (Controlled Traffic Flow): Spécifiez le flux du traffic à contrôler. Pour le protocole GRE, il n'est pas nécessaire de préciser une adresse IP ou un port. Pour les autres protocoles au moins une valeur doit être entrée.
(null) Packet type: Le type de paquet à contrôler. Pour le protocole GRE, il n'est pas nécessaire de préciser une adresse IP ou un port. Pour les autres protocoles au moins une valeur doit être entrée.

- **ANY:** Tous les types.
- **TCP**
- **UDP**
- **ICMP**
- **GRE:** Pour les connexions VPN PPTP.

Taux de Transfert assigné(Assigned Data rate): Pour déterminer le ratio de bande passante alloué à une règle. Exemple, nous voulons attribuer 20% de la bande totale pour le Serveur FTP en direction LAN vers WAN.Il faut entrer la valeur = 20. Si vous avez une ligne ADSL 256Kbps, le débit estimé est de 20% * 256 * 0.9 = 46kbps (0.9 est le facteur estimé pour le débit réel LAN vers WAN d'une ligne ADSL. Pour WAN vers LAN, le facteur est de 0.8 à 0.85).

Ratio(Data Ratio): Pourcentage du débit attribué.

Type de Transfer(Rate Type): 2 types existants:

- **Fixed (Maximum):** Pour fixer le taux maximum de transfert à une règle.

- **Guaranteed (Minimum):** Pour fixer le taux minimum de transfert à une règle, la fonction suivante permet d'en accroitre la bande passante en affectant une priorité à la règle .

Priorité à la bande passante libre (Priority for Non-used Bandwidth): Si une partie de la bande passante utilisable n'est pas affectée à une règle, il est possible d'en « récupérer » une partie grâce à cette fonction. Il suffit de préciser le niveau de priorité de chacune des règles.

- **Haut(High)**
- **Normal: Correspond à une priorité normale.**
- **Bas(Low)**

Marquage DSCP LAN vers WAN (DSCP Marking): Differentiated Services Code Point (DSCP), les 6 premiers bits duToS. DSCP Marking permet de classifier le traffic en utilisant la table DSCP pour envoyer les paquets.

DSCP Mapping Table	
Disabled	Non activé
Best Effort	Très rapide (000000)
Premium	Rapide (101110)
Gold service (L)	Classe 1, Gold (001010)
Gold service (M)	Classe 1, Silver (001100)
Gold service (H)	Classe 1, Bronze (001110)
Silver service (L)	Classe 2, Gold (010010)
Silver service (M)	Classe 2, Silver (010100)
Silver service (H)	Classe 2, Bronze (010110)
Bronze service (L)	Classe 3, Gold (011010)
Bronze service (M)	Classe 3, Silver (011100)
Bronze service (H)	Classe 3, Bronze (011110)

- **IPs des machines locales (Local Machine Ips)**: L'adresse IP du PC de votre réseau local que vous voulez contrôler.Pour les paquets LAN vers WAN, l'adresse IP de la source, pour les paquets WAN vers LAN l'adresse IP de destination.
- **IPs des machines distantes (Remote Machine Ips)**: L'adresse IP du PC distant que vous voulez contrôler.Pour les paquets LAN vers WAN, l'adresse IP de destination, pour les paquets WAN vers LAN l'adresse IP de la source.

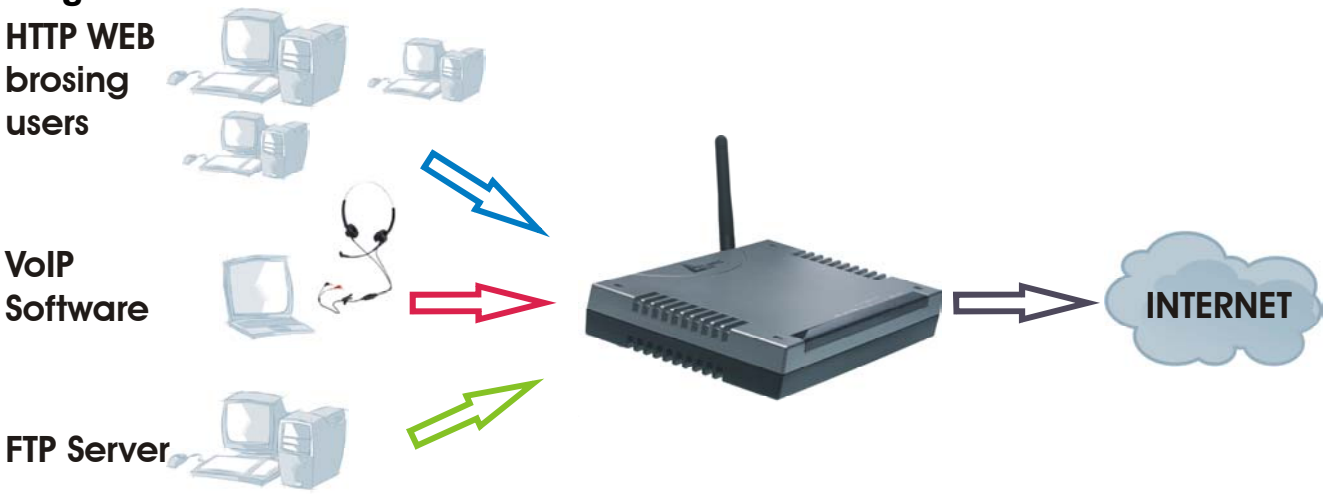
- **Ports Locaux des applications (Local Application Ports):** Le port de l'application du PC de votre réseau local que vous voulez contrôler. Pour les paquets TCP/UDP LAN vers WAN, le port source, pour les paquets WAN vers LAN, le port destination.

- **Ports distants des applications (Remote Application Ports):** Le port de l'application du PC distant que vous voulez contrôler. Pour les paquets TCP/UDP LAN vers WAN, le port destination, pour les paquets WAN vers LAN, le port source.

Horaire programmé (Schedule Time): Programmation des règles du QOS.

Exemple de QOS pour votre réseau

Diagramme de Connection



Débit de votre ligne ADSL

Montant: 256 kbps
Descendant: 1024 Mbps

Example de plan QOS

Application	IP ou Ports	Flux de Contrôle	Taux de transfert	Durée
VoIP	192.168.1.1	Sortant	Minimum 20% avec haute priorité pour la bande non utilisée (SDCP Classe 1 Service Gold)	Toujours
Serveur FTP	192.168.1.100	Entrant et Sortant	Sortant : minimum 30% Entrant : minimum 30% Les deux avec une priorité basse	Fonction de 9:00 à 18:00 H du Lundi au Vendredi.
Utilisateurs HTTP	80	Entrant et Sortant	Sortant : limité à 20% Entrant : limité à 30%	Toujours

Example de Setup QOS

QoS

Maximum ISP Bandwidth

Type: Manual Input	Upstream(LAN->WAN): 256 Kbps	Downstream(WAN->LAN): 1024 Kbps

QoS Rule List

	Application	Time Schedule	Direction	Assigned Bandwidth Ratio
○	VoIP	Always On	LAN to WAN	20% (46kbps) Minimum Guaranteed Rate with High priority
○	FTP_Server_Out	Day Time	LAN to WAN	30% (69kbps) Minimum Guaranteed Rate with Low priority
○	FTP_Server_IN	Day Time	WAN to LAN	30% (261kbps) Minimum Guaranteed Rate with Low priority
○	HTTP_Out	Always On	LAN to WAN	20% (46kbps) Fixed Rate
◉	HTTP_IN	Always On	WAN to LAN	30% (261kbps) Fixed Rate

Non-Assigned Bandwidth Ratio

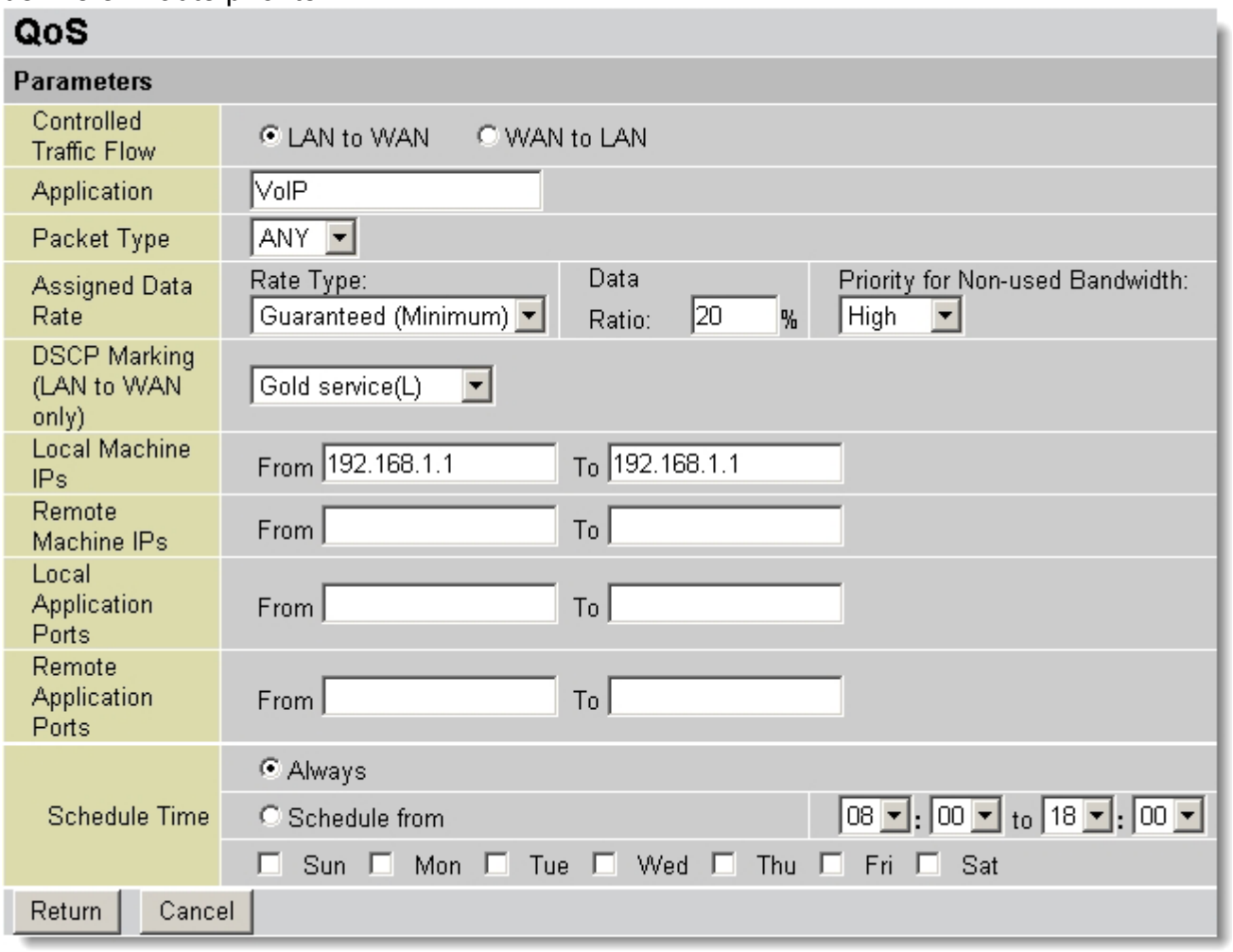
	LAN to WAN : **30%**	WAN to LAN : **40%**

Add Edit Delete

Apply Cancel

Application VoIP

Application sensible ou la plupart des appareils VoIP utilise le protocole SIP, le port est automatiquement assigné par le module SIP. Il est préferable d'utiliser une adresse IP fixe définie en haute priorité.

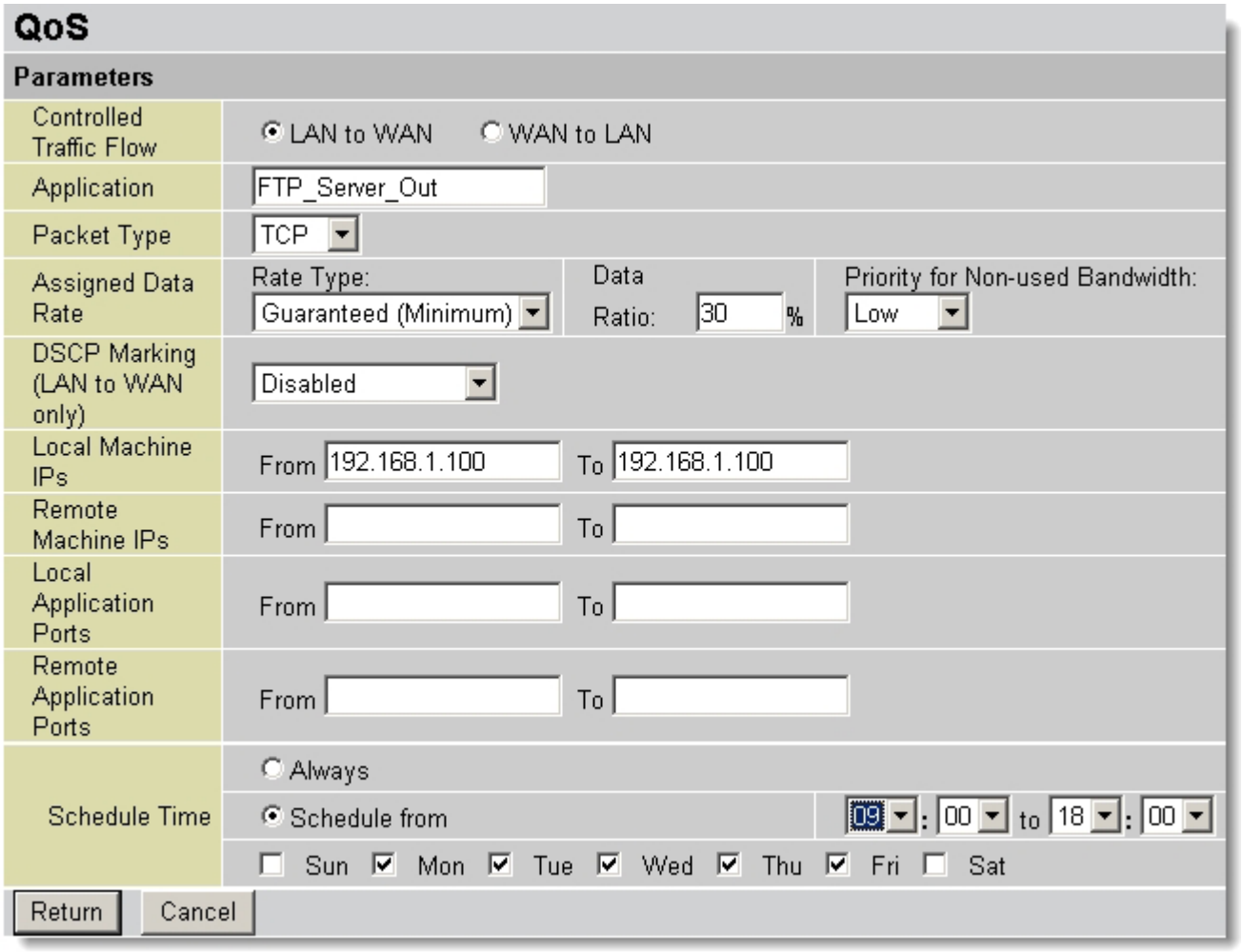


La fenêtre ci-dessus vous montre les réglages qui optimisent le service VOIP lorsque le traffic est important.

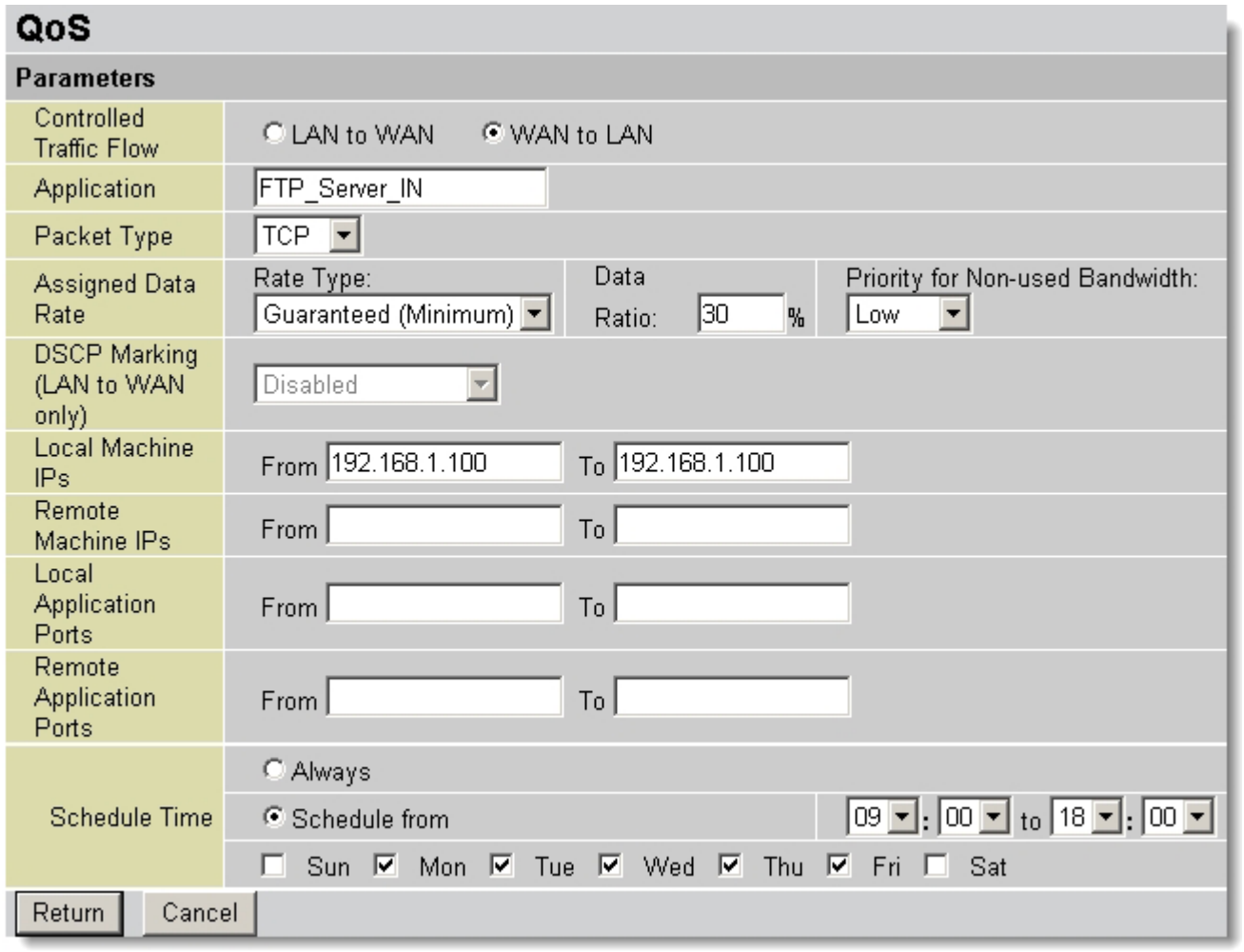
Application de Serveur FTP

De nombreuses sociétés utilisent un serveur FTP pour permettre à leurs clients le téléchargement de données et quelques particuliers pour partager des fichiers.

Direction LAN vers WAN:



Direction WAN vers LAN:

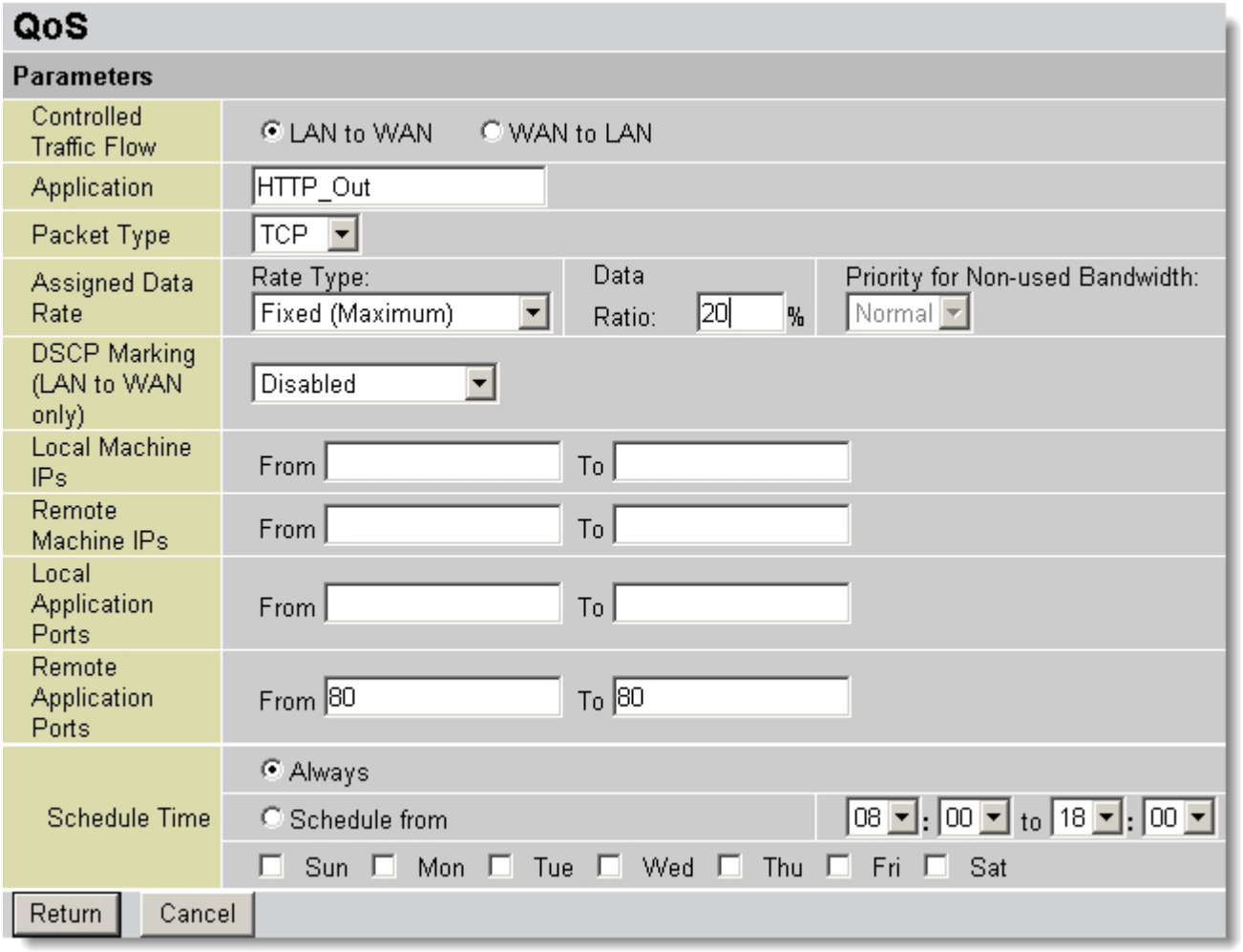


La fenêtre ci-dessus vous permet de limiter la bande passante disponible et défini les horaires d'utilisation.

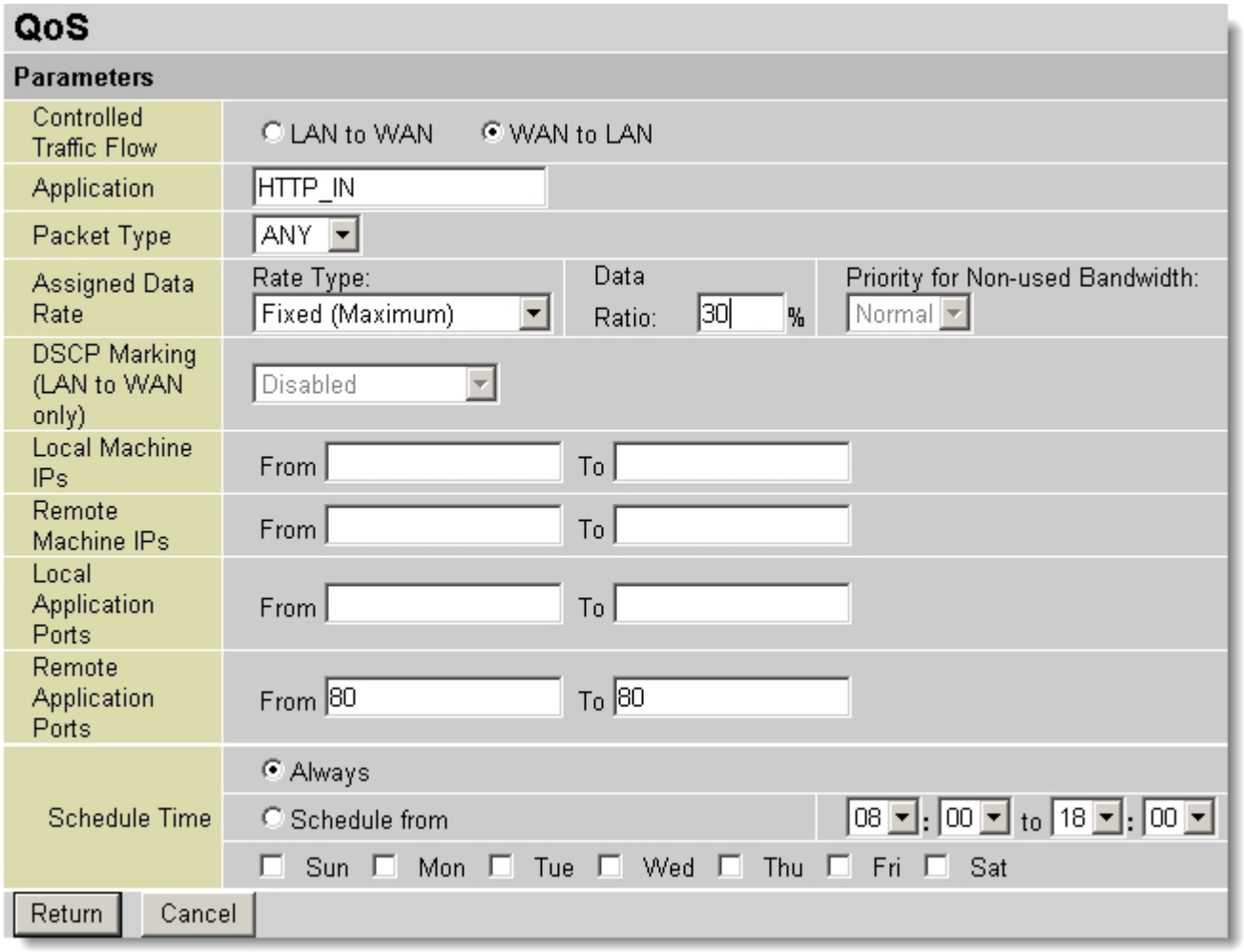
Utilisateurs HTTP

Vous pouvez controler la navigation sur Internet en spécifiant les règles du port HTTP 80 (8080 pour certain serveur proxy).

Direction LAN vers WAN:

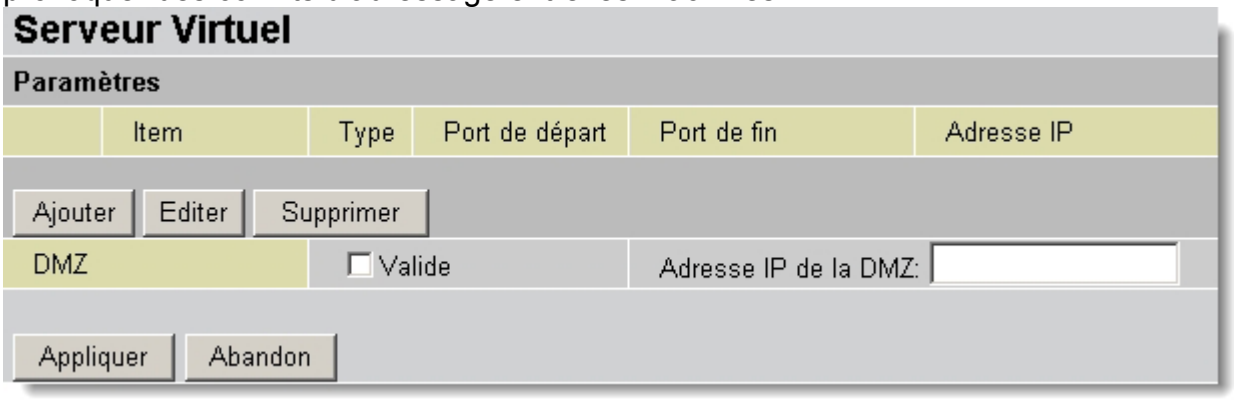


Direction WAN vers LAN:

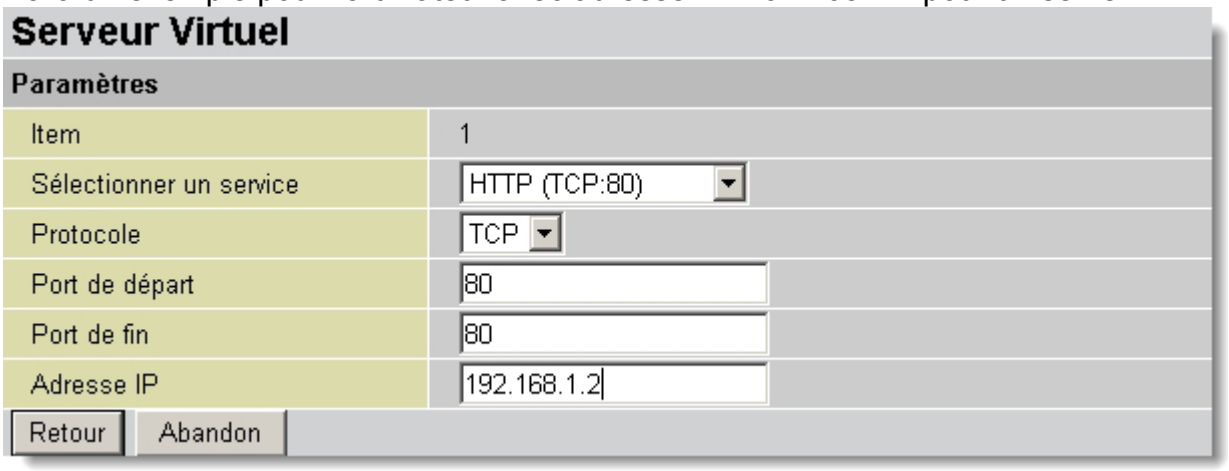


3.6.3.6 Serveur Virtuel

Cet écran vous permet d'ouvrir les ports et de configurer les accès depuis Internet à des serveurs localisés sur votre réseau local, en toute sécurité. Si vous installez des serveurs sur votre réseau local, veillez à ne pas inclure leurs adresses IP dans la plage d'adresses distribuées par le serveur DHCP (utilisez la modalité Fixed Host). Vous risqueriez de provoquer des conflits d'adressage entre les machines.



Voilà un exemple pour l'ordinateur avec adresse IP=192.168.1.2 pour un server WEB



Vous devez choisir le protocole (éventuellement les ports pour TCP/UDP) et l'adresse IP de l'ordinateur hébergeant le serveur.

Pour utiliser certains logiciels spécifiques vous devez paramétrer la section Virtual Server.

Logiciels	Sortie	Entrée
ICQ 98, 99a	N/A	N/A
NetMeeting 2.1 a 3.01	N/A	1503 TCP, 1720 TCP
VDO Live	N/A	N/A
mIRC	N/A	N/A
Cu-SeeMe	7648 TCP &UDP, 24032 UDP	7648 TCP &UDP, 24032 UDP
PC AnyWhere	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP
Edonkey/Emule	N/A	Essentiellement 4660-4662 TCP , 4665 UDP
MSN Messenger	N/A	TCP da 6891-6900 TCP 1863 TCP 6901 UDP 1863 UDP 6901

		UDP 5190
VNC	N/A	TCP 5900

Liste des Ports les plus utilisés :

Type de serveurs	Numéro de port
File Transfer Protocol (FTP) Data	20/tcp
FTP Commands	21/tcp
Telnet	23/tcp
Simple Mail Transfer Protocol (SMTP) Email	25/tcp
Domain Name Server (DNS)	53/tcp and 53/udp
Trivial File Transfer Protocol (TFTP)	69/udp
finger	79/tcp
World Wide Web (HTTP)	80/tcp
POP3 Email	110/tcp
SUN Remote Procedure Call (RPC)	111/udp
Network News Transfer Protocol (NNTP)	119/tcp
Network Time Protocol (NTP)	123/tcp and 123/udp
News	144/tcp
Simple Management Network Protocol (SNMP)	161/udp
SNMP (traps)	162/udp
Border Gateway Protocol (BGP)	179/tcp
Secure HTTP (HTTPS)	443/tcp
rlogin	513/tcp
rexec	514/tcp
talk	517/tcp and 517/udp
ntalk	518/tcp and 518/udp
Open Windows	2000/tcp and 2000/udp
Network File System (NFS)	2049/tcp
X11	6000/tcp and 6000/udp
Routing Information Protocol (RIP)	520/udp
Layer 2 Tunnelling Protocol (L2TP)	1701/udp

DMZ: permet la redirection de tous les protocoles vers une adresse déterminée du Reseau. Peut être utilisé pour permettre le passage de services déterminés. Evidemment l'utilisation d'une DMZ est une faille pour la sécurité, il ne faut l'utiliser que pour des raisons précises. Insérer dans le champ DMZ l'adresse IP du PC sur lequel on souhaite établir la DMZ.

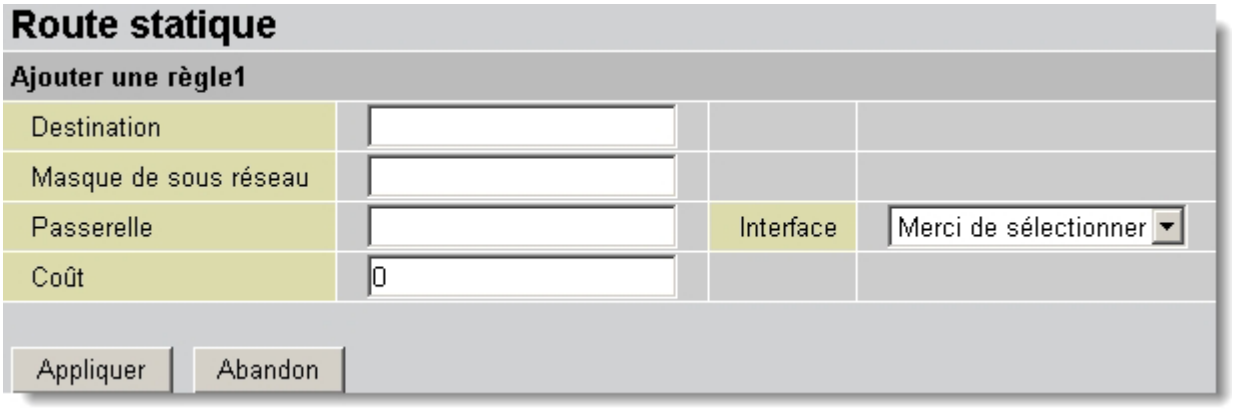
3.6.3.7 Fonctions avancées

Dans cette section, vous pouvez accéder à la configuration avancée du routeur:

- **Route Statique(Static Route)**
- **DNS Dynamique (Dynamic DNS)**
- **Contrôle du Vlan (VLAN Control)**
- **Gestion du matériel (Device Management)**
- **IGMP**

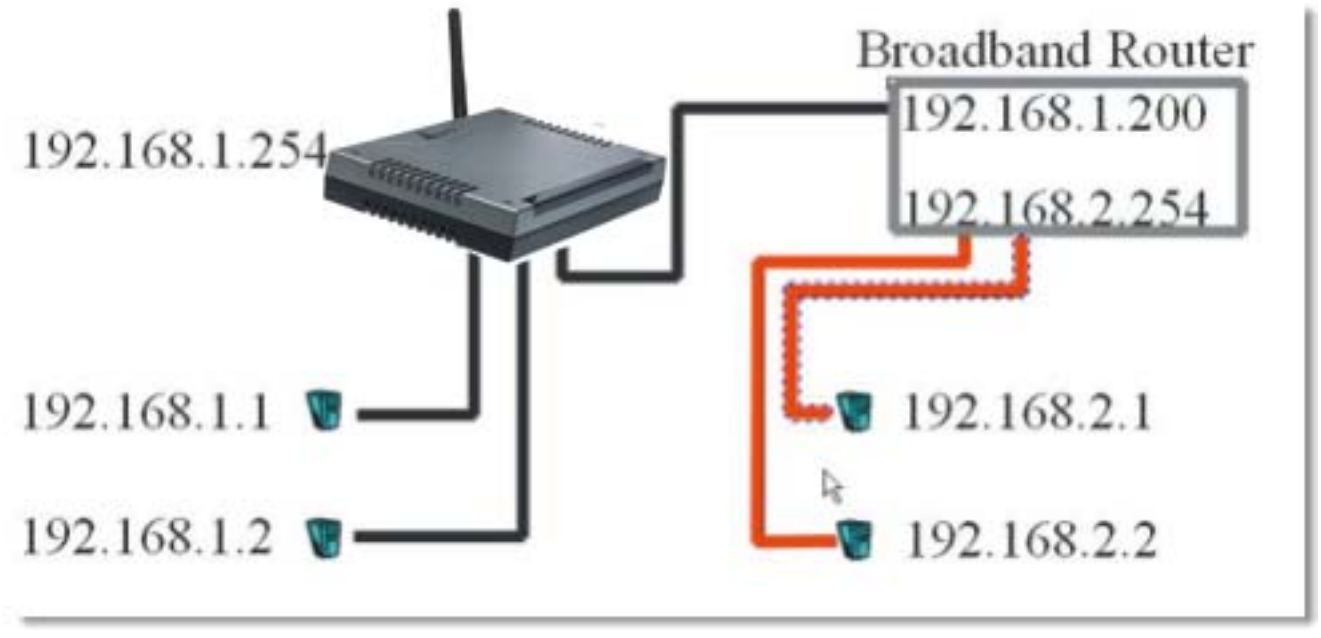
3.6.3.7.1 Route Statique(Static Route)

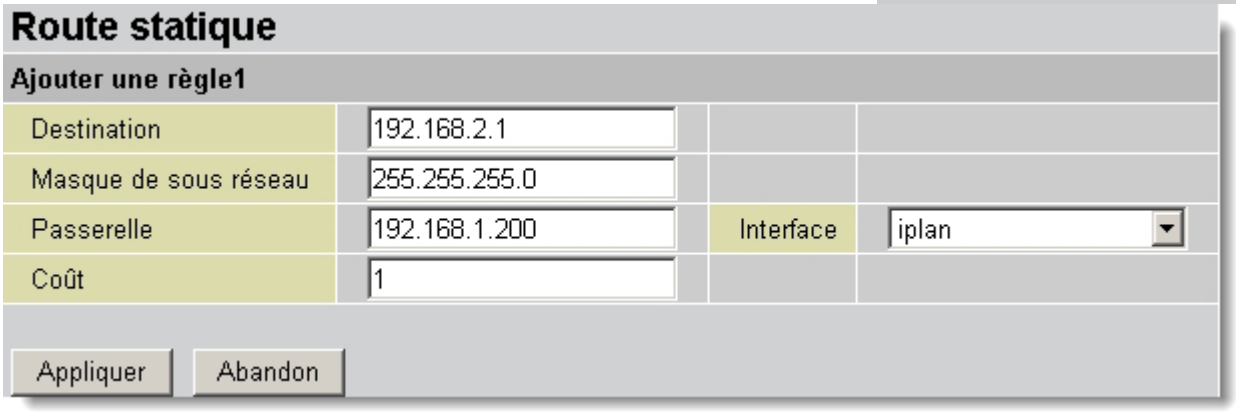
Si vous avez un autre Routeur BroadBand sur le LAN, vous devez introduire une ligne dans le tableau.



- **Destination:** L'adresse IP de destination.
- **Masque de sous Réseau(Netmask):** Le masque de sous réseau de destination.
- **Passerelle(Gateway):** La passerelle par défaut ou les paquets doivent être acheminés.
- **Coût(Cost):** en général 1.
- **Interface:** Entrer l'interface ou les paquets doivent être acheminés.

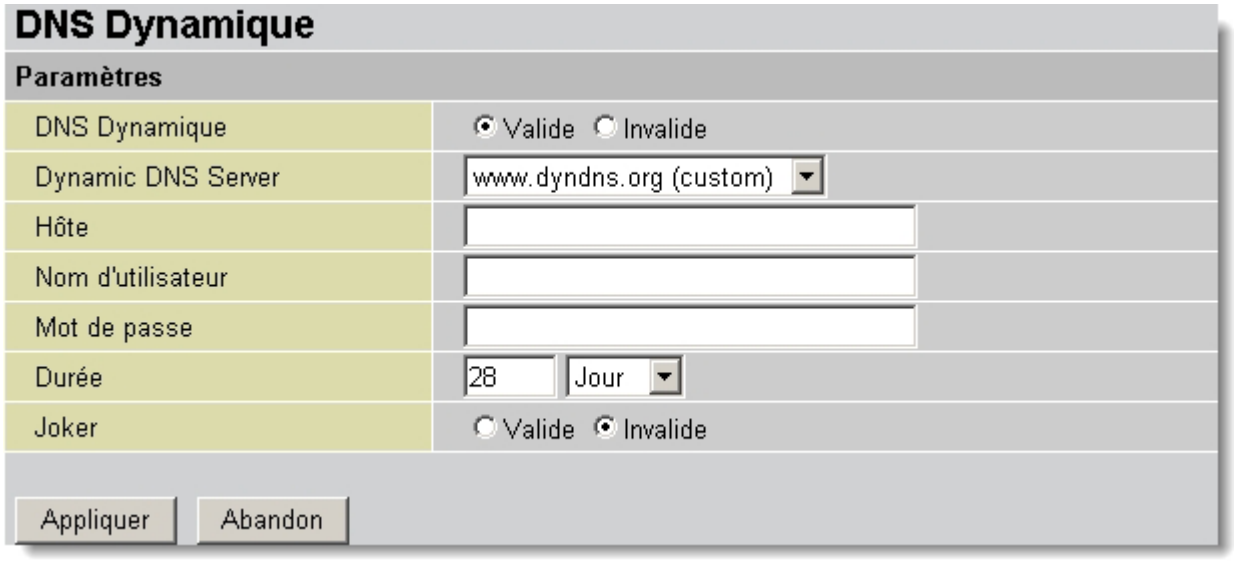
Exemple de configuration :





3.6. 3.7.2 DNS Dynamique (Dynamic DNS)

Vous devez introduire les données pour que le Routeur ajourne le server DDNS avec la nouvelle adresse IP.



Ces nouveaux services vous permettent de créer un nom de domaine sur un serveur DNS auquel sera affecté l'adresse IP actuelle de votre Routeur mais surtout de prévenir ce serveur DNS que votre Routeur à changer d'adresse IP et qu'il faut donc l'actualiser avec l'adresse IP du nom de domaine en question.

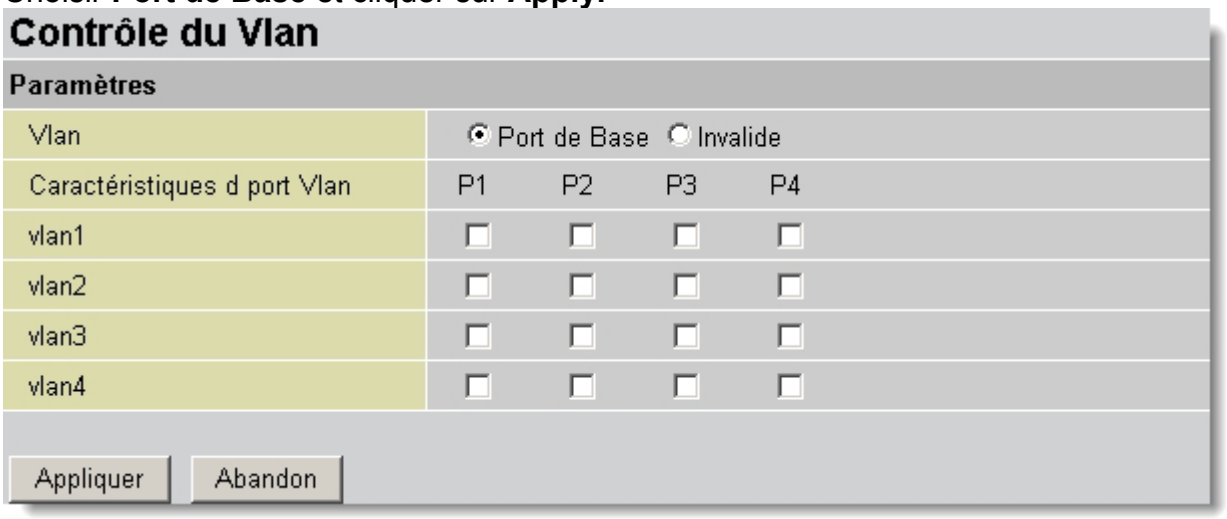
- Enregistrer un nom de domaine gratuitement et instantanément sur **www.dyndns.org**, **www.zoneedit.com**.
- Vous devez correctement paramétrer le client dans le Routeur (**Username**, **Password**, **Domain Name** et **Dynamic DNS**)

Pour de plus amples détails, lisez l'appendice A.

3.6.3.7.3 Contrôle du Vlan (Contrôle VLAN)

Le VLAN permet de segmenter le trafic du réseau en améliorant sa gestion et surtout ses performances. De plus il augmente la sécurité globale du réseau LAN. Chaque VLAN est en effet constitué d'un nombre arbitraire de ports (qui peuvent appartenir à des VLAN différents). Il est donc possible de créer des sous-réseaux qui ne peuvent communiquer qu'en fonction des réglages éffectués par l'administrateur.
Sécurité: Les données sont confinées dans le seul VLAN d'appartenance, d'où une diminution des d'utilisateurs pouvant examiner le trafic réseau.
Limitation des coûts: Permet de créer des domaines multiples sans utiliser de routeur.
L'appareil gère le VLAN sur la base des ports.

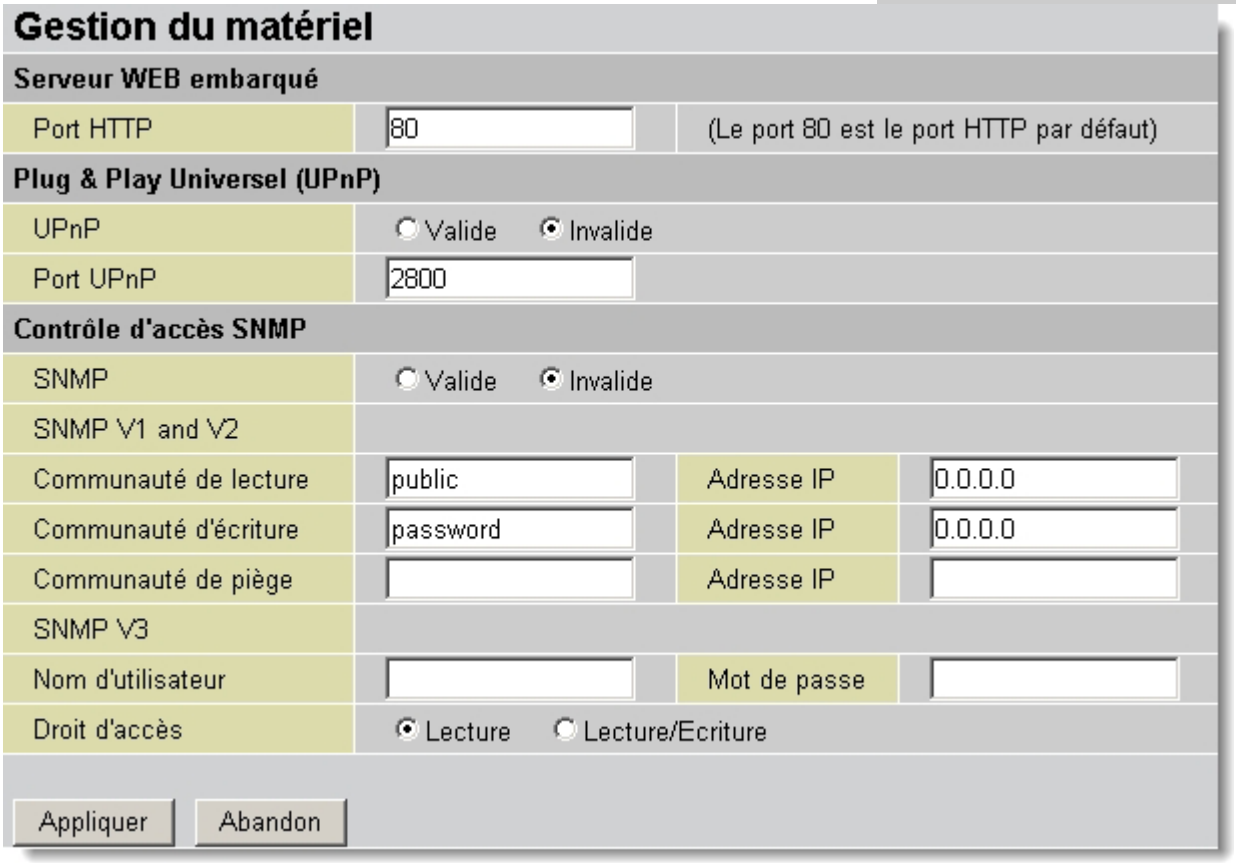
Choisir **Port de Base** et cliquer sur **Apply.**



Vous pouvez créer des groupes VLAN, composés par des ports qui forment des sous-réseaux indépendants. Pour ajouter un VLAN, il suffit d'ajouter les ports et cliquer sur **Appliquer(Apply).**

3.6.3.7.4 Gestion du matériel (Device Management)

Dans cette section, vous pouvez choisir le port de configuration du Routeur, activer le protocole UpnP (Pour de plus amples détails, consulter l'appendice D) et le SNMP.



Simple Network Management Protocol (SNMP) est un protocole qui peut être activé sur votre Routeur. Il sert à la gestion des réseaux, principalement pour l'administrateur. Plusieurs composants constituent la structure SNMP, agents, gestion du réseau (NMS), protocoles de gestion du réseau et une base d'information de la gestion (MIB). Un agent SNMP est typiquement un noeud résidant sur votre réseau (ordinateur ou routeur). L'agent SNMP est contrôlé et configuré par le NMS en envoyant des messages SNMP entre eux. Les agents SNMP sont connectés et identifiés dans une Base de Gestion de l'Information (MIB) dans laquelle leurs sont attribués des identificateurs d'objet (OID).
Une fonction de SNMP est de créer des traces qui sont utilisées pour notifier à l'administrateur réseau, les événements importants qui ont eu lieu sur le réseau.
Ces traces sont envoyées au SNMP NMS (le Serveur NMS localise l'IP du Piège) à travers les ports spécifiés.
SNMP Système Identification:
Communauté de lecture(Read Community): Mot de passe pour accéder à l'information publique (maximum 127 caractères), par défaut “public” .
Communauté d’écriture (Write Community): Mot de passe pour accéder à l'information privée (maximum 127 caractères), par défaut “private”.
Communauté de piège (Trap Community): Mot de passe pour accéder aux vues des traces SNMP (maximum 127 caractères), par défaut “trap community”
Trap SNMP Version: Sélectionnez la Version 1 ou 2, par défaut Version 1
Trap IP: C'est l'adresse IP à laquelle les traces SNMP sont envoyées, il peut y en avoir jusqu'à 5
Trap Port: C'est le port correspondant à l'IP du Trap
SNMP Version: SNMPv2c and SNMPv3
Le dispositif inclut les TRAPs suivantes**: Cold Start, Authentication Failure.**
Le dispositif inclut les MIBs suivants**:**

- **RFC 1213 (MIB-II):**
  System group

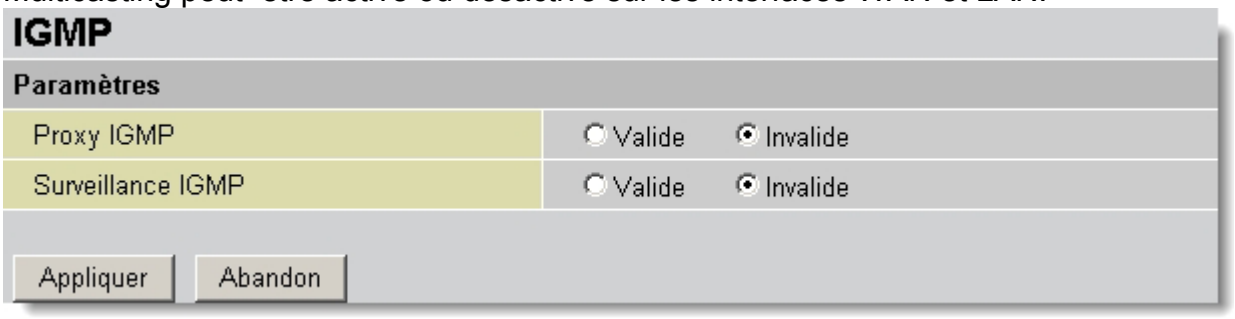
Interfaces group
Address Translation group
IP group
ICMP group
TCP group
UDP group
EGP (not applicable)
Transmission
SNMP group

- **RFC1650 (EtherLike-MIB):**
  dot3Stats
- **RFC 1493 (Bridge MIB):**
  dot1dBase group
  dot1dTp group
  dot1dStp group (if configured as spanning tree)
- **RFC 1471 (PPP/LCP MIB):**
  pppLink group
  pppLqr group
- **RFC 1472 (PPP/Security MIB):**
  PPP Security Group)
- **RFC 1473 (PPP/IP MIB):**
  PPP IP Group
- **RFC 1474 (PPP/Bridge MIB):**
  PPP Bridge Group
- **RFC1573 (IfMIB):**
  ifMIBObjects Group
- **RFC1695 (atmMIB):**
  atmMIBObjects
- **RFC 1907 (SNMPv2):**
  only snmpSetSerialNo OID

3.6.3.7.5 IGMP

Traditionnellement les paquets IP sont transmis en Unicast (1 expéditeur – 1 destinataire) ou en Broadcast (1 expéditeur – tout le réseau). Le Multicast permet d'envoyer les paquets à un groupe défini de clients sur le réseau.
L'IGMP (Internet Group Multicast Protocol) est un protocole utilisé pour établir une relation d'appartenance dans un groupe Multicast – il n'est pas utilisé pour transporter les données.
L'IGMP version 2 (RFC 2236) est une évolution de la version 1 (RFC 1112), mais ce dernier est encore très utilisé. Pour plus de détails sur l'interopérabilité entre les protocoles IGMP version 1 et 2, consultez les sections 4 et 5 de l'RFC 2236. Les adresses IP de classe D sont utilisées pour identifier un groupe de clients et se trouvent dans la plage (224.0.0.0 à 239.255.255.255).
L'adresse IP 224.0.0.0 n'est assignée à aucun groupe mais est utilisée par les ordinateurs avec IP Multicast. L'adresse 224.0.0.1 est utilisée pour les requêtes et est assignée à toutes les adresses IP, incluant les passerelles par défaut. Les clients doivent appartenir au groupe 224.0.0.1 pour participer à la communication IGMP. Le Wireless Router ADSL2+ supporte les deux versions du protocole IGMP. Au démarrage, le Wireless Router ADSL2+ interroge tous les réseaux qui lui sont connectés pour identifier les appartenances de groupe.

Ensuite, le Wireless Router ADSL2+ met à jour périodiquement ces informations. L'IP Multicasting peut être activé ou désactivé sur les interfaces WAN et LAN.



3.6.4 Sauvegarde en mémoire (Save Config to Flash)

Permet de sauvegarder chaque changement de configuration, sur la mémoire du routeur (eprom), Cliquer sur **Sauvegarde en mémoire (Save Config to Flash)** puis sur **Appliquer (Apply)**.

Chapitre 4
Problèmes

Lorsque le Wireless Router ADSL2+ ne fonctionne pas correctement, avant de vous adressez au service après vente ou à votre FAI, consultez ce chapitre.

Problèmes au démarrage du Wireless ADSL Router

Problème	Actions correctives
Aucune LED n'est allumée lorsqu'on connecte le Wireless Router ADSL2+ au réseau électrique.	Contrôlez la connexion entre l'alimentation et le Router ADSL. Assurez-vous que le Power Switch est sur la position ON. Si le problème persiste, adressez-vous au support technique d'Atlantis Land.

Mot de passe?

Problème	Actions correctives
Password et/ou IP oublié.	Il est possible, en perdant la configuration, de reseter l'appareil en appuyant (au moins 10 secondes) sur le bouton Reset, situé à l'arrière du Routeur. Lorsque le routeur est allumé, pressez pour effectuer le reset ou le restore jusqu'à ce que les LEDS cessent de clignoter puis éffectuer un redemarrage par la touche Power On/Off.

Impossible d'entrer dans le Router par le WEB

Problème	Actions correctives
En appelant l'IP par défaut du Router (192.168.1.254), via le navigateur Internet, on n'obtient aucune réponse.	Le problème peut être du, soit à un câblage inapproprié soit à cause d'une adresse IP incorrecte. Vérifiez le câblage (il ne doit pas y avoir de problème en cas de connexion directe entre l'ordinateur et le Router, grâce à la fonction d'auto polarité il fonctionne avec des câbles droits ou croisés. Il peut par contre y en avoir si on utilise un Hub ou Switch sans auto-polarité. Effectuez un Ping vers l'IP du Router, s'il ne répond pas il faut contrôler l'adresse IP de l'ordinateur (introduisez WINIPCFG pour Win95/98/ME ou IPCONFIG pour WIN2000/NT/XP) et le déplacez sur la classe 192.168.1.x (par exemple 192.168.1.1, Masque de sous réseau 255.255.255.0 et passerelle par défaut, l'adresse du Router).

Problèmes avec l'interface LAN

Problème	Actions correctives
Il n'est pas possible de faire un ping avec un ordinateur du LAN.	Contrôlez la LED LAN, sur le panneau avant. Elle devrait être allumée (au moins une des 4) sinon contrôlez le câblage.
	Vérifiez, dans le cas ou la LED est allumée, que l'adresse IP et le masque de sous réseau entre le Router et les ordinateurs sont corrects.

Problèmes avec l'interface WAN

Problème	Actions correctives
L'initialisation de la connexion ne fonctionne pas.	Assurez vous que le câble RJ11 est connecté correctement à la ligne téléphonique et au Wireless Router ADSL2+. La LED ADSL doit être allumée et fixe. Lorsqu'elle clignote, attendez qu'elle se stabilise, la connexion n'est pas réalisable autrement. Contrôlez les valeurs de VPI et VCI, le type de codification et le type de modulation (valeurs fournies par l'ISP). Relancez le Wireless Router ADSL2+. Allez (avec le PPPoA/PPPoE) dans **Status** et contrôlez l'état de la connexion. Lorsque le problème persiste, contactez l'ISP et vérifiez ces paramètres.

Problèmes de Connexion à un Noeud distant ou à un FAI

Problème	Actions correctives
Le Router ne peut pas se connecter.	Vérifiez dans Status, l'ADSL pour voir l'état de la ligne.
	Vérifier Login et Password pour la connexion en PPPoA/PPPoE. Contrôlez l'adresse IP dans le cas de RFC1483.
	Contrôlez le type de codification utilisée et les valeurs de VCI/VPI (si vous avez des doutes, supprimez la connexion et utilisez la procédure de Quick Start).

Conflits d'adresses IP

Problème	Actions correctives
L'ordinateur montre un message informant d'un conflit d'adresse IP.	Le Wireless Router ADSL2+ est en réamorçage (si configuré comme serveur DHCP) ou au moins deux ordinateurs ont la même adresse. Il est possible, en exécutant **winipcfg** ou **ipconfig**, de contrôler tous les paramètres (IP, Subnet, Passerelle par défaut) et éventuellement les renouveler (si l'ordinateur est un client DHCP et le Router agit comme serveur DHCP).

Le Router ne peut pas se positionner?

Problème	Actions correctives
La Led ADSL continue de clignoter et le Wireless Router ADSL2+ n'arrive pas à se positionner.	Le Router, grâce au support du protocole G.994.1 (G.hs), peut choisir le type de modulation automatiquement. Il peut être nécessaire de forcer un type de modulation (glite, gdmt, multi, ansi etc).

Qu'est ce que le NAT?

Demande	Réponse
Que fait exactement le NAT?	Nat signifie Network Address Translation (translation des adresses du réseau local). Il a été proposé et décrit dans l'RFC-1631 et il avait, au moins au début, la tâche de permettre une exploitation intensive des adresses IP. Chaque appareil supportant le NAT est composé d'un tableau basé sur des couples d'adresse IP (privée et publique). Le Router Wireless ADSL supporte le NAT, plusieurs utilisateurs peuvent accéder à Internet en utilisant un seul compte (et une seule IP publique). Si les utilisateurs du réseau ont des adresses IP publiques et peuvent donc accéder directement à Internet, cette fonction doit être désactivée. Le Nat agit comme premier pare-feu en améliorant la sécurité du réseau local. Cette fonction n'entre pas en conflit avec les fonctions Virtual Server, DMZ et DHCP. Le Nat manipule les paquets IP sortants et il change le champ **IP expéditeur** (dans ce cas l'adresse IP de l'ordinateur qui est une IP privée non valide Internet) avec l'IP publique du Wireless ADSL Router. De cette façon tous les paquets sortants du Router auront dans le champ expéditeur l'adresse IP publique du Router. Puis, quand les paquets reviennent au Routeur, grâce aux tableaux sauvegardés, ils seront renvoyés à l'ordinateur émetteur.

Paquets IP

Problème	Actions correctives
Ne fonctionne pas sur un ordinateur du réseau local.	Le Router ADSL applique, à chaque paquet, dans l'ordre: • Virtual Server • Pare-feu • DMZ Pour que la DMZ fonctionne, il faut s'assurer qu'il n'y a aucun bloc avant (Pare-feu) ou (Virtual Serveur) qui ne travaille de manière incorrecte. Positionnez l'ordinateur qui agit comme un serveur avec une adresse IP privée fixe (ou utiliser le mode Fixed Host en DHCP).

Une application Internet ne fonctionne pas correctement

Problème	**Actions correctives**
Quelques applications, quand le Wireless Router ADSL2+ est configuré en NAT et/ou pare-feu, peuvent ne pas fonctionner correctement.	Le Wireless Router ADSL2+, à travers le NAT et/ou le pare-feu, protége le réseau en l'isolant de l'extérieur et en refusant toutes connexions entrantes. Sur Internet chaque service est associé à un port, ces ports doivent être fermés pour éviter que des personnes mal intentionnées puissent accéder au réseau. Cependant, il est nécessaire pour le bon fonctionnement de certaines applications (par exemple NetMeeting), que les tentatives de connexions entrantes sur des ports déterminés soient renvoyées à un ordinateur du réseau sur lequel le programme soit en "écoute". Consultez la section Virtual Server pour avoir plus de détails. Les applications typiques devant être configurées ainsi sont par exemple: • Certains Programmes d'Email • Des jeux Multi Joueurs • Des Applications de conférence Audio/Vidéo Pour trouver les numéros des ports à ouvrir pour chaque application, consultez le site web de son éditeur. Un seul ordinateur du réseau pourra utiliser cette application.

Pourquoi même avec le Serveur Virtuel des applications ne marchent pas?

Problème	Actions correctives
Même en effectuant l'affectation des ports avec le VS, l'application ne fonctionne pas correctement.	Il peut être nécessaire d'effectuer une DMZ vers l'ordinateur sur lequel on veut lancer une application particulière.

Pourquoi même avec le DMZ des applications ne marchent pas?

Problème	Actions correctives
Même en utilisant la DMZ, l'application ne fonctionne toujours pas.	Malgré les caractéristiques avancées du Router, des applications peuvent ne pas fonctionner parce que non compatibles avec le NAT (même en effectuant une DMZ). Dans ce cas il faut utiliser le Wireless Router ADSL2+ en modalité Bridge. De cette façon, l'adresse IP publique du Router est donnée à l'ordinateur qui pourra faire fonctionner toutes les applications (comme si le Router était un modem ADSL). Demander à l'ISP le protocole PPPoE puis configurer le Router selon le protocole RFC1483 Bridge, de cette manière un seul ordinateur (doté d'un client PPPoE) pourra accéder à Internet.

RFC 1483 Bridge avec MAC OS 9

Problème	Solution
En ayant un abonnement de type PPPoE, il est possible d'utiliser le Router en modalité RFC 1483 Bridge avec une machine Mac OS9.	Le **MacPoet** est un logiciel PPPoverEthernet, compatible avec tout les MacOS. Après avoir téléchargé le fichier, lancez l'installation, une fois terminée allez en TCP/IP et contrôlez que dans le champ **Connecte Par** soit sélectionné **Ethernet Built-in. C**liquez sur l'icône MacPoeT, une fenêtre apparaîtra, il suffit d'introduire le username et le mot de passe fourni par le FAI et de cliquez sur **Connecte**. Pour lancer la connexion, après avoir ouvert MacPoet, il suffit de sélectionner **Connecte au Startup**.

RFC 1483 Bridge avec MAC OS X

Problème	Solution
En ayant un abonnement de type PPPoE, il est possible d'utiliser le Router en modalité RFC 1483 Bridge avec une machine MAC OS X.	De la même manière que Microsoft Windows XP, Apple Mac OSX a une potentialité intéressante permettant de créer une connexion Internet à travers le protocole PPP over Ethernet sans devoir installer de composants supplémentaires La configuration de la connexion est très simple: Cliquez sur **Préférences de système,** puis sur **Network**. Dans la fenêtre **Network,** pour **Configure** sélectionnez **ETHERNET INTEGREE,** puis cliquez sur **PPPoE** et introduisez les données fournies par votre FAI. Si nécessaire, cliquez sur "TCP/IP" pour introduire les DNS. Cliquez enfin sur **Registre** pour sauvegarder les modifications. La connexion en PPPoE a été crée. Pour lancer la connexion il suffit d'aller dans le menu **VAIS**, **Applications**, **Connexion Internet**, **Configuration**, **Ethernet Intégrée**, **CONNEXION**.

RFC 1483 Bridge avec Windows 95, 98, ME

Problème	Solution
En ayant un abonnement de type PPPoE, il est possible d'utiliser le Router en modalité RFC 1483 Bridge avec une machine avec Windows 95, 98, ME.	Il est possible d'utiliser n'importe quel logiciel (Ethernet, Win PoET, RasPPPoE). Les instructions pour RasPPPoE (freeware) sont ci-dessous. Placez les différents fichiers (en version décompactée) du logiciel dans un répertoire. Double cliquez sur **Panneau de contrôle, Réseau, Ajout**, **Protocole, Ajout**. Sélectionnez **Disque Driver**, sélectionnez le répertoire où ont été placé les pilotes puis choisissez n'importe lequel des trois fichiers .inf, cliquez sur **OK** et redémarrez la machine. Pour créer la connexion, allez dans **C:\Windows\System et** cliquez deux fois sur le fichier **raspppoe.exe**. Dans la fenêtre, sélectionnez la carte réseau à laquelle le Router est connecté, puis cliquez sur **Créer une connexion Dial-Up pour l'Adaptateur sélectionné** et enfin choisissez **exit**. L'installation est terminée, une icône a été crée, il suffira de la cliquer pour lancer la connexion à internet.

RFC 1483 Bridge avec Windows 2000

Problème	Solution
En ayant un abonnement de type PPPoE, il est possible d'utiliser le Router en modalité RFC 1483 Bridge avec une machine avec Windows2000.	Mêmes démarches que pour Windows 95/98/Me sauf chemin de lancement du programme **C:\Windows2000\System32.**

RFC 1483 Bridge avec LINUX

Problème	Solution
En ayant un abonnement de type PPPoE, il est possible d'utiliser le Router en modalité RFC 1483 Bridge avec une machine Linux.	Pour Linux il est nécessaire d'installer un logiciel appelé Roaming's Pinguins. Pour de plus amples détails sur la configuration, se référer à la documentation jointe au logiciel.

Les performances du Router ne sont pas bonnes

Problème	Actions correctives
Les performances obtenues ne sont pas les mêmes que celles indiquées sur le contrat de votre l'ISP.	Assurez-vous que le câble ADSL est partout à au moins 30cm de n'importe quelle source d'alimentation. Positionnez le Wireless Router ADSL2+ loin de tout appareil susceptible de générer des champs électromagnétiques (ordinateurs avec le capot ouvert, monitor CRT, téléphones mobiles). Si l'on n'obtient pas le résultat désiré, contrôlez votre contrat pour **la bande minimale garantie** et éventuellement contactez votre FAI. Si les problèmes persistent, contactez l'assistance technique d'Atlantis Land .

Qu'est ce que le relais DHCP ?

Demande	Réponse

Qu'est ce que le Relais DHCP ?	En activant cette fonction le service DHCP traverse le Router Wireless pour se connecter au serveur DHCP du réseau qui attribue les différentes adresses IP. Si cette fonction n'est pas activée, des ordinateurs pourraient ne pas accéder au serveur DHCP. Habituellement chaque ordinateur qui nécessite une adresse IP, contacte un serveur DHCP et reçoit automatiquement: IP, Masque de sous réseau, Passerelle par défaut et DNS. Ces adresses IP sont dynamiques, c'est à dire qu'elles ont une durée de validité, quand celle-ci cesse le client DHCP contacte de nouveau le serveur pour obtenir une nouvelle adresse IP et/ou un nouveau bail.

Qu'est ce que c'est le temps de mise au repos?

Demande	Réponse
À quoi sert l'IDLE Time?	Le router ADSL interrompt la connexion, s'il n'y a pas de trafic sur la connexion pendant un temps exprimé en minutes (aucun paquet n'a été adressé du Router vers Internet).

Pourquoi le Wireless Router ADSL2+ se connecte automatiquement à l'ISP?

Demande	Réponse
Pourquoi le Wireless Router ADSL2+ se connecte automatiquement au FAI?	Le Wireless Router ADSL2+ génère une connexion quand un ordinateur du réseau envoi un paquet (fonction de Dial on Demand) adressé à un IP différent de celui de sa classe d'appartenance.

Qu’est ce qu’une attaque de Deni de Service?

Demande	Réponse
Qu’est ce qu’une attaque Denial of Service?	Le but de ces attaques est d’obtenir des informations particulières du réseau plutôt que de le rendre inutilisable. Plus précisément il en existe 4 types. 1-Attaques qui ont pour but de congestionner la bande passante, elles sont réalisées de deux manières. En solo ou lorsque la bande passante est plus grande que celle qui attaque, elle peut être saturée en utilisant d’autres hosts qui amplifient l’attaque. 2-Attaques qui ont comme but de congestionner les ressources. 3-Attaques contre des défauts de programmation, qui ont comme but d’exploiter des bug logiciel ou matériel. 4-Attaques DoS génériques. Le Router peut automatiquement relever et bloquer une attaque de type DoS (Denial of Service) si cette fonction est activée.

Comment empêcher à un groupe d'utilisateurs de surfer sur Internet?

Demande	Réponse
Comment empêcher à un groupe d'utilisateurs de surfer sur Internet pendant que d'autres ont un accès total ?	**Utiliser le MAC Filter :** il faut connaître l'adresse MAC des ordinateurs d'un des deux groupes puis fixez les règles d'accès au routeur. **Utiliser Packet Filter - Address Filter** Il faut assigner aux ordinateurs qu'on veut limiter, des adresses IP fixes en désactivant leur client DHCP (on peut utiliser la fonction Fixed Host, mais il est nécessaire de connaître les adresses Mac). De cette manière, en ayant toujours les mêmes adresses IP, il devient possible de suivre le schéma ci-après: Les utilisateurs qui appartiennent au **group A** seront filtrés, ceux du **group B** auront au contraire un accès sans aucune limitation à tout les services Internet (compatibles avec le niveau de sécurité configuré). Choisissez dans le pare-feu du Wireless Router ADSL2+ la politique DROP et introduisez des règles pour faire sortir toutes les adresses IP du groupe B.

Qu’est ce que le DDNS?

Demande	Réponse
À quoi sert le DDNS ?	À travers cette fonction il devient possible d’enregistrer un nom de domaine et de l’associer à une adresse IP dynamique. Chaque fois que le Router se connectera, à travers le client incorporé, il communiquera au serveur DNS la nouvelle adresse IP. En associant cette fonction avec le Virtual Server, vous pouvez (par exemple) héberger un site WEB sur votre ordinateur, effectuer des configurations à distance et utiliser le Router comme serveur VPN. Les passages à suivre sont les suivants: • Enregistrez votre propre domaine (par exemple) gratuitement www.dyndns.org, www.zoneedit.com. L’opération demande quelques minutes. • Configurez le client sur le Wireless Router ADSL2+ en introduisant les champs appropriés (Domain Name, Username et Password). Attention à la configuration du champ Period (le Router met à jour le serveur DDNS en utilisant comme paramètre le champ Period, en outre à chaque fois qu’il reçoit de PPPoA/PPPoE une nouvelle adresse IP) en respectant les règles du gérant DDNS. • Configurez l’ordinateur pour la fonction de Server Web ou configurez le Router pour pouvoir l'administrer à distance ou comme serveur VPN. • Configurez le Virtual Server avec l’adresse l’IP de l’ordinateur (décrit ci-dessus), prédisposé aux connexions entrantes De cette manière chaque utilisateur, qui veut se connecter à l’adresse enregistrée, interrogera le serveur DDNS qui lui donnera l’adresse IP assignée par le Router du FAI. En utilisant la fonction de connexion (disponible en PPPoA et PPPoE) lorsque la connexion tombe, le Router l’activera de nouveau immédiatement. Le serveur WEB sera donc toujours disponible sur Internet.

Est-ce que je peux démarrer une application d'un ordinateur satellite présent dans le réseau wireless??

Demande	Réponse
Est-ce que je peux démarrer une application d'un ordinateur satellite présent dans le réseau wireless?	Ça dépende directement de l'application même ; s'elle a été projetée pour travailler en réseau(n'import si wireless ou câblée) il n'y aura aucun problème..

Est –ce que je peux jouer en réseau avec les autres ordinateurs présents dans le WLAN?

Demande	Réponse
Est –ce que je peux jouer en réseau avec les autres ordinateurs présents dans le WLAN?	Oui, si le jeu est doué de la fonctionnalité multi-joueur en réseau.

Qu'est-ce que c'est le Spread Spectrum?

Demande	Réponse
Qu'est-ce que c'est le Spread Spectrum?	La transmission Spread Spectrum est basée sur la dispersion de l'information sur une bande beaucoup plus ample de celle nécessaire à la modulation du signal disponible. L'avantage qu'on obtient avec cette technique de modulation est en fait une basse sensibilité aux bruits radioélectriques même pour transmissions à puissance limitée. Cette caractéristique est clairement précieuse quand on doit transmettre des données.

Qu’est-ce que c'est DSSS et FHHS?

Demande	Réponse
Qu’est-ce que c'est DSSS et FHHS?	DSSS (Direct-Sequence Spread-Spectrum): C’est une particulière technologie de transmission pour la large bande qui permet de transmettre chaque bit d’une façon redondante. C’est adapte particulièrement ù la transmission et à la réception de signaux faibles. FHHS (Frequency Hopping Spread Spectrum): C’est une technologie qui permet le partage entre plusieurs utilisateurs d’un même ensemble de fréquences. Pour empêcher interférences entre périphériques du même type les fréquences de transmission changent jusqu’à 1.600 fois chaque second.

Peuvent les informations envoyées par wireless être interceptées?

Demande	Réponse
Peuvent les informations envoyées par wireless être interceptées?	Le Wireless Multi-Function offre la fonctionnalité de cryptage WEP jusqu’à 128 bits ; ce permet des transmissions des données wireless plus sures.

Qu’est-ce que c’est WEP?

Demande	Réponse
Qu’est-ce que c’est WEP?	WEP est le sigle de Wired Equivalent Privacy, un protocole de sécurité pour les réseaux locaux sans fils (WLAN) défini par le standard 802.11b.

Qu’est-ce que c’est infrastructure mode?

Demande	Réponse
Qu’est-ce que c’est infrastructure mode?	Dans la configuration Infrastructure un réseau WLAN et un réseau WAN communiquent entre eux à travers un access point.

Qu’est-ce que c’est ISM band?

Demande	Réponse
Qu’est-ce que c’est ISM band?	Cette fréquence a été mise à disposition par la FCC, après la requête des entreprises qui voulaient développer des solutions wireless pour l’usage civil de chaque jour ; elle est généralement caractérisée par le sigle ISM band (Industrial, Scientific and Medical). En cette fréquence ils travaillent seulement des dispositifs industriels, scientifiques et médicales à une basse puissance.

Qu’est-ce que c’est le standard IEEE 802.11g?

Demande	Réponse
Qu’est-ce que c’est le standard IEEE 802.11g?	Le nouveau standard 802.11g travaille à la fréquence de 2,4 Ghz et donc il est totalement compatible avec la plus diffue b. L’avantage est qu’il permet une vitesse de transfert de 54 Mbps, cinq fois supérieure au standard 802.11b.

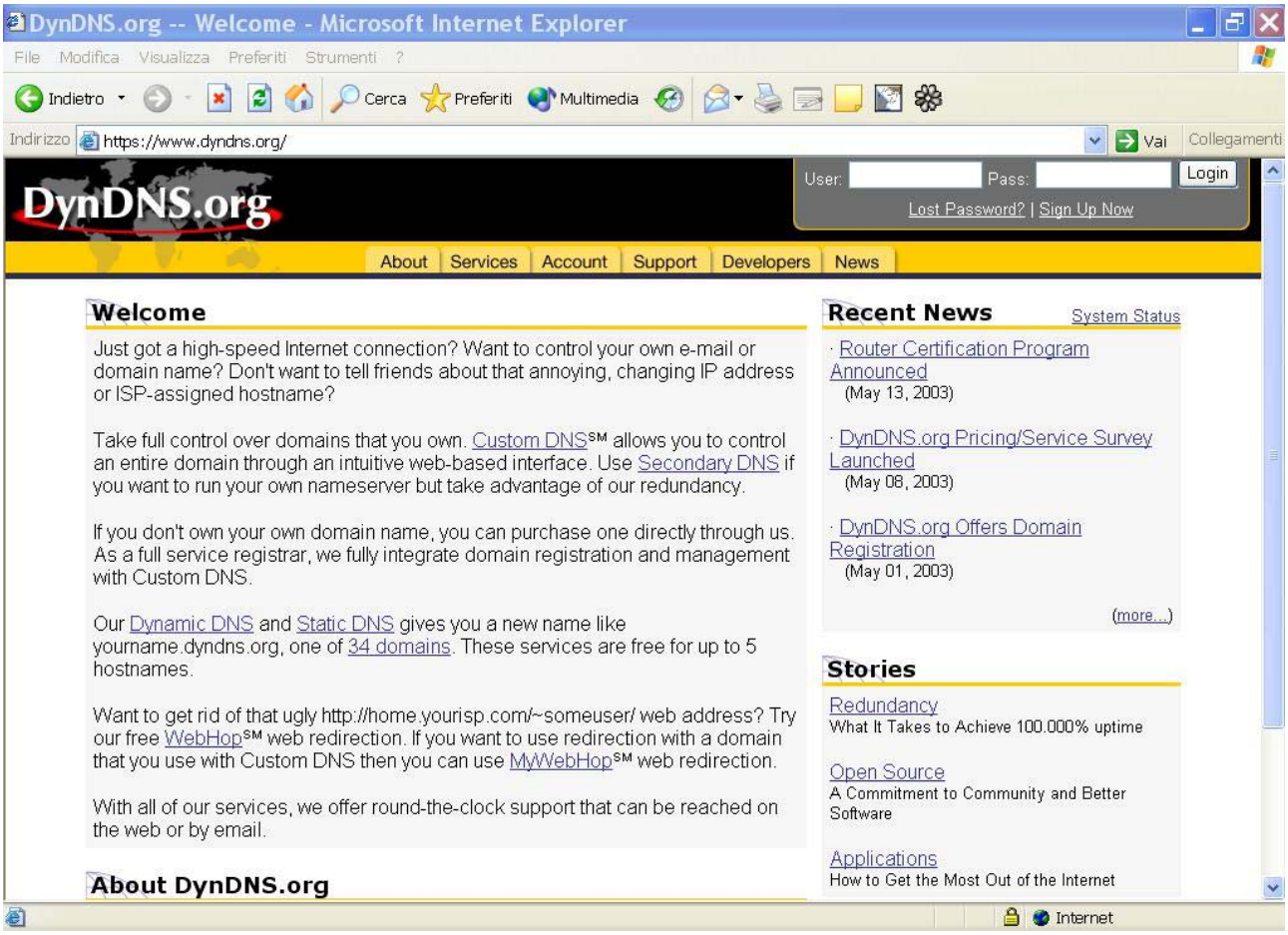
Toutes les marques citées appartiennent à leurs propriétaires respectifs.

APPENDICE A

Dynamique DNS

Grâce à ce service, vous pouvez enregistrer un nom de domaine, même associé à une adresse IP dynamique. Il y a de nombreux serveurs DDNS qui offrent gratuitement ce type de fonction. Il suffit de s'enregistrer pour activer immédiatement le service, qui vous permettra de joindre le Wireless Router ADSL2+ de l'extérieur. Vous pourrez de cette façon, effectuer facilement la configuration à distance, héberger votre site WEB ou utiliser le Router comme serveur VPN.
Chaque fois que le Wireless Router ADSL2+ se connectera, il communiquera au serveur DDNS la nouvelle adresse IP. De cette manière, les accès extérieurs à votre URL, fonctionneront sans avoir à connaitre l'adresse IP assignée au Router.
Voyons en détail comme effectuer un enregistrement avec un administrateur DDNS, peut-être le plus connu.

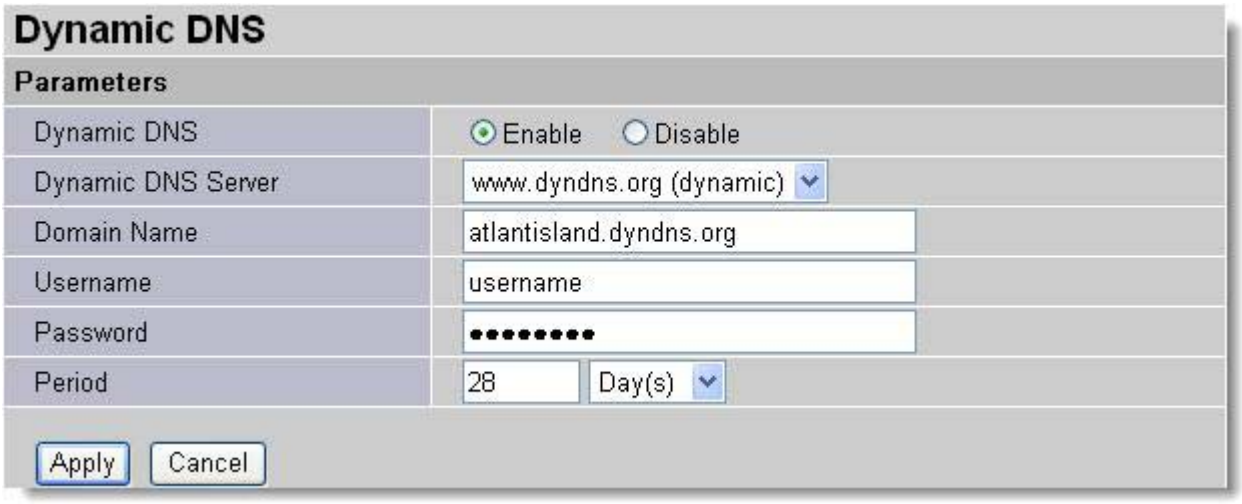
Allez sur le site:www.dyndns.org, cliquez sur **Account.**


DynDNS.org -- Welcome - Microsoft Internet Explorer
https://www.dyndns.org/
DynDNS.org
User:
Pass:
Login
Lost Password? | Sign Up Now
About
Services
Account
Support
Developers
News
Welcome
Just got a high-speed Internet connection? Want to control your own e-mail or domain name? Don't want to tell friends about that annoying, changing IP address or ISP-assigned hostname?
Take full control over domains that you own. Custom DNS℠ allows you to control an entire domain through an intuitive web-based interface. Use Secondary DNS if you want to run your own nameserver but take advantage of our redundancy.
If you don't own your own domain name, you can purchase one directly through us. As a full service registrar, we fully integrate domain registration and management with Custom DNS.
Our Dynamic DNS and Static DNS gives you a new name like yourname.dyndns.org, one of 34 domains. These services are free for up to 5 hostnames.
Want to get rid of that ugly http://home.yourisp.com/~someuser/ web address? Try our free WebHop℠ web redirection. If you want to use redirection with a domain that you use with Custom DNS then you can use MyWebHop℠ web redirection.
With all of our services, we offer round-the-clock support that can be reached on the web or by email.
About DynDNS.org
Recent News
System Status
· Router Certification Program Announced
(May 13, 2003)
· DynDNS.org Pricing/Service Survey Launched
(May 08, 2003)
· DynDNS.org Offers Domain Registration
(May 01, 2003)
(more...)
Stories
Redundancy
What It Takes to Achieve 100.000% uptime
Open Source
A Commitment to Community and Better Software
Applications
How to Get the Most Out of the Internet
Internet

Effectuez l'enregistrement en cliquant sur **Create Account,** puis en introduisant: **Username, Adresse Mail et Password.**

Il vous sera immédiatement envoyé un e-mail avec les instructions permettant de continuer. Suivez les en remplissant le formulaire pour terminer cette phase.

Entrez de nouveau dans le site, allez sur **Services**, mettez en évidence (dans la partie gauche) le menu **Dynamic DNS,** puis cliquez sur **Add Host**.
Il ne vous reste plus qu'à introduire le **Nom de l'host,** mettez en évidence Enable WildCard, choisissez le suffixe que vous souhaitez, puis appuyez sur le bouton **Add Host** pour terminer.
Pour finir, il faut introduire les données pour que le Routeur ajourne le server DDNS avec la nouvelle adresse IP.



APPENDICE B

Filtrage de paquets

Le Router possède un système sophistiqué de Packet Filter qu'il utilise pour examiner le trafic qui le traverse. De cette manière, il est possible en connaissant les caractéristiques des paquets IP associés aux services les plus communs, d'effectuer les filtrages de façon correcte. Dans cet appendice, on verra comment les paquets d'un service peuvent changer. On utilisera les conventions suivantes:

- **BLEU** pour indiquer une INVERSION
- **ROUGE** pour indiquer un CHANGEMENT

Pour mieux comprendre les changements qu'un paquet IP subit, imaginons les conditions suivantes:

- NAT actif
- PC(X) de la LAN avec IP 192.168.1.X
- Router avec LAN IP 192.168.1.254

On considère le cas ou le PC(X) veuille voir un site WEB. On va suivre en détail les paquets, pendant les différentes étapes.

Il y a 2 phases: résolution de l'URL (cette valeur pourrait être récupérée en cache ou fournie par des programmes appropriés) et construction de la connexion TCP avec le site WEB.

Le premier paquet est envoyé par le PC(X) (avec IP 192.168.1.X) vers le serveur DNS pour demander la résolution de l'URL cherchée.

	Direction Paquet	ordinateur-Router[Sortant]	
IP	IP Expéditeur	192.168.1.X	
	IP Destination	IP du Server DNS	
	Paquet contenu	Type UDP	UDP
	Port Expéditeur	C	
	Port Destination	53	

Ce paquet sortant arrive au Router qui le NAT étant activé, en change l'adresse de l'expéditeur en y mettant son adresse Publique et le renvoi au serveur DNS.

	Direction Paquet	Router-Internet[Sortant]	
IP	IP Expéditeur	**IP coté WAN du Router**	
	IP Destination	IP du Server DNS	
	Paquet contenu	Type UDP	UDP
	Porte Expéditeur	C	
	Porte Destination	53	

Arrivé au serveur DNS, le paquet retourne au Router, y sont intervertis au niveau IP, les champs expéditeur et destination, au niveau UDP les ports.

	Direction Paquet	Internet-Router[Entrante]	
IP	IP Expéditeur	**IP du Server DNS**	
	IP Destination	**IP coté WAN du Router**	
	Paquet contenu	Type UDP	UDP
	Porte Expéditeur	**53**	
	Porte Destination	**C**	

Arrivé au Router, le paquet est examiné et envoyé à l'IP de début.

	Direction Paquet	Internet-Router[Entrante]	
IP	IP Expéditeur	IP du Server DNS	
	IP Destination	**192.168.1.X**	
	Paquet contenu	Type UDP	UDP
	Porte Expéditeur	53	
	Porte Destination	C	

À ce point, à travers le paquet UDP arrivé, le PC(X) (192.168.1.X) a résolu l'URL et il connaît l'adresse IP associée. Commence donc la phase de construction de la connexion TCP (le protocole TCP en faisant la demande, contrairement à UDP).

	Direction Paquet	ordinateur-Router[Sortant]	
IP	IP Expéditeur	192.168.1.X	
	IP Destination	IP URL	
	Paquet contenu	Type TCP	TCP
	Porte Expéditeur	K	
	Porte Destination	80	

Ce paquet sortant arrive au Router qui le NAT étant activé, en change l'adresse de l'expéditeur en y mettant son adresse Publique et le renvoi au serveur WEB.

	Direction Paquet	Router-Internet[Sortant]	
	IP Expéditeur	**IP coté WAN du Router**	
	IP Destination	IP URL	
	Paquet contenu	Type TCP	
	Porte Expéditeur	K	

	Porte Destination	80	P

Arrivé au serveur WEB, le paquet retourne au Router, y sont intervertis au niveau IP, les champs expéditeur et destination, au niveau TCP les ports.

	Direction Paquet	Internet- Router [Entrante]	
I P	IP Expéditeur	**IP URL**	
	IP Destination	**IP coté WAN du Router**	
	Paquet contenu	Type TCP	T C P
	Porte Expéditeur	**80**	
	Porte Destination	**K**	

Arrivé au Router, le paquet est examiné et renvoyé à l'IP de l'expéditeur.

	Direction Paquet	Router- ordinateur[Entrante]	
I P	IP Expéditeur	IP URL	
	IP Destination	**192.168.1.X**	
	Paquet contenu	Type TCP	T C P
	Porte Expéditeur	80	
	Porte Destination	K	

On a vu le parcours des paquets et leurs différentes transformations. Dans l'exemple en haut on a utilisé des paramètres C et K. Ce sont des nombres entiers >1024. Dans les protocoles de ports TCP/UDP en fait l'expéditeur parle à un port de destination (sur lequel on écoute le serveur) et il indique un port (le port de l'expéditeur) où il attend la réponse. Le paquet, une fois reçu par le serveur, est renvoyé à l'expéditeur sur le port ou la réponse est attendue. Au niveau IP, le même parcours est effectué.

APPENDICE C

Considérations sur les réseaux Sans Fil (Wireless)

Cette section decrit les réseaux sans fils (Wireless Lan) et quelques configurations de base. Un Wireless Lan peut être crée simplement avec deux ordinateurs dotés de cartes réseau Wireless ; ils communiquent dans un réseau «peer-to-peer» ou d'une façon plus complexe en utilisant plusieurs ordinateurs avec cartes réseau Wireless ; les cartes réseau communiquent à travers un point d'accès qui agit comme un pont entre le réseau Wireless et le réseau câblé.

Canaux
La plage de radio fréquences, utilisée par les appareils Wireless IEEE802.11b et IEEE802.11g est partagée en "canaux". Le spectre des communications Wireless va de 2.412Ghz jusqu'à 2.472 Ghz. Le nombre de canaux disponibles dépend de la zone géographique. Il est donc possible de sélectionner des canaux différents pour éliminer d'éventuelles interférences avec les Point d'Accès proches. L'interférence se constate lorsque deux ou plusieurs canaux s'interposent en diminuant les performances; cette situation est appelée "Overlap".
On conseille de maintenir une marge de 5 canaux entre deux utilisés (ex. AP1-canal 1, AP2-canal 6).

ESS ID
L'Extended Service Set (ESS) consiste en un groupe de Point d'Accès ou Gateway Wireless connecté à un LAN câblé sur le même subnet. Un ESS ID identifie uniquement chaque groupe. Chaque Access Point ou Gateway Wireless et les stations Wireless associées doivent avoir le même ESSID.
Il est possible d'envoyer en broadcast l'ESSID (en permettant à n'importe qui de se connecter à l'AP) ou de bloquer le broadcast (en permettant seulement aux utilisateurs qui ont déjà l'ESSID de se connecter).

Niveau de Sécurité
Les fonctions de Wireless Security sont nécessaires pour protéger les communications entre les stations Wireless, les Points d'Accès et le réseau câblé.
Le tableau ci-dessous indique les différents niveaux de sécurité Wireless fournis par le Router ADSL. Le niveau de sécurité le plus haut est basé sur le protocole EAP (Extensible Authéntication Protocol) pour authentifier et utilise WEP avec échange de clés dynamiques. Ce système demande l'interaction avec un serveur RADIUS (Remote Authéntication Dial-In User Service) qui offre des services d'authentification pour stations Wireless.
Si aucune fonction de sécurité n'est utilisée, il est possible d'accéder au Routeur de n'importe quelle station Wireless présente dans son rayon d'action. On peut configurer ce service à travers l'interface de configuration Web du produit.
Le protocole WAP PSK est la dernière évolution en ce qui concerne la sécurité et grâce à l'intégration du TKIP et MIC, il rend les communications wireless très sures.

Codification des données avec WEP/WPA

La codification WEP fournit le cryptage des données transmises sur le réseau pour obtenir une communication sécurisée. Le cryptage est effectué sur les communications unicast et multicast.

Toutes les stations Wireless qui utilisent cette codification doivent utiliser la même clé pour le codage et le décodage des données. Le Wireless Router ADSL2+ est capable d'utiliser des clés de cryptage de 64 et 128 bits.

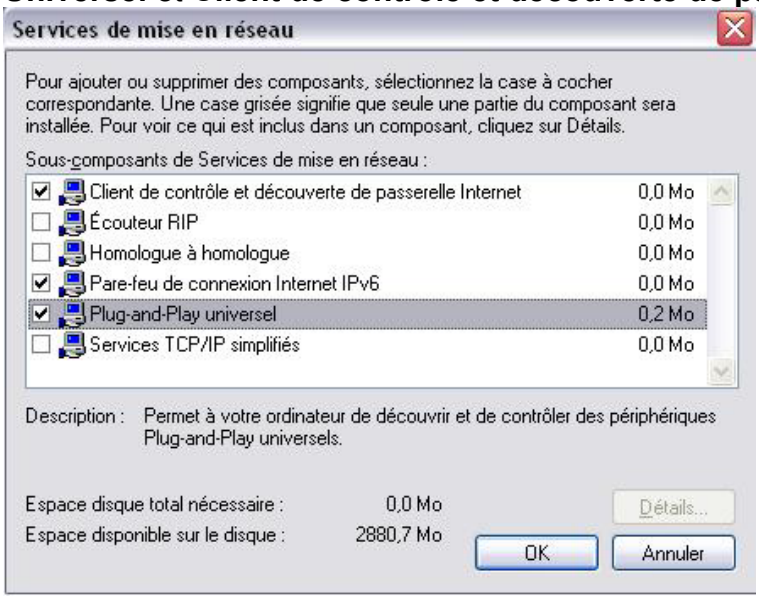
Le tableau suivant décrit les champs contenus dans la section "Wireless".

Paramètre	Description
ESSID	Introduisez une description (maximum de 32 caractères).
Hide ESSID	Sélectionnez Enable pour cacher l'ESSID, de cette façon une station Wireless ne peut pas obtenir l'ESSID à travers un scan passif. Sélectionnez Disable pour rendre visible l'ESSID, de cette façon une station Wireless peut l'obtenir.
Canal ID	Sélectionnez le canal désiré.
Codification WEP	Sélectionnez "Disable" pour permettre une communication sans aucun codage (aucune sécurité). Sélectionnez 64-bits WEP ou 128-bits pour utiliser la fonction de codage souhaitée
Clé 1 à 4	Les clés WEP sont utilisées pour le cryptage des données. Toutes les stations Wireless qui doivent communiquer entre elles, doivent utiliser la même clé. Si on sélectionne 64-bits WEP, introduisez 5 caractères ASCII ou 10 caractères hexadécimaux ("0-9", "A-F"). Si on sélectionne 128-bits WEP, introduisez 13 caractères ASCII ou 26 caractères hexadécimaux. On ne peut activer qu'une seule clé à la fois
WAP PSK	Introduisez la clé partagée, commune à tous les clients, composée d'un minimum de 8 caractères et d'un maximum de 63
TKIP	Introduisez l'intervalle temps en seconde, après lequel le dispositif effectue la mise à jour automatique des clés.

APPENDICE D

Universel PnP

Grâce à la fonction UpnP, vous pourrez configurer facilement toutes les applications qui ont des problèmes pour traverser le NAT. L'usage de U-PNP rendra les applications capables de se configurer automatiquement sans l'intervention de l'utilisateur. Il sera donc aisé, sans connaîssances particulières, d'utiliser totalement les avantages du NAT et d'utiliser les applications Internet les plus communes sans problèmes.
Panneau de Contrôle puis **Ajout/Suppression de programmes**, choisissez **Ajouter ou Supprimer des composants Windows**. Sélectionnez **Services de mise Réseau,** puis cliquez sur **Détails**. Assurez-vous que les choix suivants sont sélectionnés: **Plug and Play Universel** et **Client de contrôle et découverte de passerelle Internet**


Services de mise en réseau
Pour ajouter ou supprimer des composants, sélectionnez la case à cocher correspondante. Une case grisée signifie que seule une partie du composant sera installée. Pour voir ce qui est inclus dans un composant, cliquez sur Détails.
Sous-composants de Services de mise en réseau :
Client de contrôle et découverte de passerelle Internet 0,0 Mo
Écouteur RIP 0,0 Mo
Homologue à homologue 0,0 Mo
Pare-feu de connexion Internet IPv6 0,0 Mo
Plug-and-Play universel 0,2 Mo
Services TCP/IP simplifiés 0,0 Mo
Description : Permet à votre ordinateur de découvrir et de contrôler des périphériques Plug-and-Play universels.
Espace disque total nécessaire : 0,0 Mo
Espace disponible sur le disque : 2880,7 Mo
Détails...
OK
Annuler

Sur **Panneau de Contrôle** puis **Connexions de réseau,** vous devriez trouver **Connexion Internet**. En double cliquant, vous verrez l'image suivante:

En choisissant **Propriétés,** puis **Paramètres** puis **Ajouter** vous effectuerez les configurations nécessaires à l'usage de l'UpnP.

Paramètres de service
Description du service :
Nom ou adresse IP (par exemple 192.168.0.12) de l'ordinateur hôte de ce service sur votre réseau :
Numéro du port externe de ce service :
TCP
UDP
Numéro du port interne de ce service :
OK
Annuler

Description du Service=identification
Nom ou Adresse IP = IP de l'ordinateur sur lequel est le serveur
Numéro de port externe du service = introduire le port externe (ex 80 pour http, 20-21 pour FTP)
Numéro de port interne du service = introduire port interne
Choisissez le protocole entre **UDP** ou **TCP**.
En appuyant sur OK, le protocole UpnP communiquera avec le Router.
Avec cette modalité, vous pouvez configurer un **Virtual Server** sur chaque ordinateur sans accéder au Router.
Seules quelques applications sont capables de configurer le service UpnP. Ceci rendra ces applications utilisables très facilement.
Dans les **Connexions Réseau** vous devriez trouver le nom du champ **Description du Service**. En cliquant dessus, vous entrerez dans la configuration du Router ADSL (de la même façon que quand vous introduisez l'IP dans l'URL de IE). En cliquant le bouton droit, puis Propriété vous aurez accès aux renseignements supplémentaires.

APPENDICE E

Caractéristiques Avançées

Protocole	IP, NAT, ARP, ICMP, DHCP (server, relais et client), RIP1/2 , SNMP, SNTP client, UPnP, Telnet server et IGMP
Port LAN	4 ports LAN Fast Ethernet
Port WAN	1 port WAN RJ11 pour la connection ADSL
Bouton	Marche/Arrêt et Bouton Reset
LED	9 LEDs pour pour un diagnostique immédiat
Standard ADSL	ANSI T1.413 Issue 2, ITU-T G.992.1 (Full Rate DMT), ITU-T G.992.2 (Lite DMT), ITU-T G.994.1 (Multimode) ITU G.992.3 (G.dmt.bis), ITU G.992.5 (G.dmt.bisplus)
Protocole ADSL	RFC2364 (PPPoA), RFC2516 (PPPoE) et RFC1483
Wireless	Standard IEEE802.11g et IEEE802.11b
Antenne	1 externe
ATM	ATM AAL2/AAL5 et ATM service : CBR, UBR, VBR-rt, VBR, ATM Forum UNI 3.0, 3.1 et 4.0
Pare feu / Firewall	Filtrage par Paquet, Adresse Mac et URL Prévention du Deni de service et Détection d'Intrusion
VPN	Pass Through
VLAN	Port base VLAN
QoS	LAN-WAN et WAN-LAN
Alimentation	Externe 12VDC/1A
Puissance electrique	< 10watts
Certification	CE
Dimension	180x 120 x 32 mm
Poids	<350g
Temperature de Fonctionnement	0 ~ 40 C / Humidité 10-95% (sans condensation)

APPENDICE F

Support

Pour tout problème ou renseignement (il est **IMPERATIF** de connaître au préalable les paramètres utilisés par le FAI), vous pouvez contacter l'help desk téléphonique gratuite d'Atlantis Land qui vous fournira assistance du Lundi au Vendredi de 9.00 à 13.00 et de 14.00 à 18.00. Vous pouvez aussi nous contacter par email tech-fr@atlantis-land.com

Atlantis Land France
57, Rue d'Amsterdam
75008 Paris
Email: tech-fr@atlantis-land.com
WWW: http://www.atlantis-land.fr

Important :
Pensez à consulter le site Web pour prendre connaissance d'éventuelles mises à jour des clauses de garantie.